



DigitPA

IL NUOVO CODICE DELL'AMMINISTRAZIONE DIGITALE

Cosa cambia per i cittadini e le amministrazioni

Il miglioramento dei rapporti di cittadini e imprese con la Pubblica Amministrazione non è solo l'attuazione di diritti fondamentali, ma dispiega i suoi effetti sulla produttività del paese e fa crescere la trasparenza e la correttezza dell'azione amministrativa. La riforma del Codice dell'Amministrazione Digitale definisce azioni concrete, obblighi e scadenze perché si realizzi un reale miglioramento nei servizi erogati dalla PA, nell'organizzazione delle amministrazioni e nella loro capacità di interagire.

IL NUOVO CODICE DELL'AMMINISTRAZIONE DIGITALE

Cosa cambia per i cittadini e le amministrazioni

SOMMARIO

PREMESSA	3
IL CAMBIAMENTO PER CITTADINI E IMPRESE	7
Elementi generali dell'innovazione digitale	8
Documenti informatici e loro validità	8
Conservazione digitale dei documenti	10
Identità digitale e trasmissione digitale dei documenti	11
L'innovazione digitale nei rapporti con l'amministrazione	14
Contenuto dei siti pubblici: informazione e trasparenza	15
Tracciabilità dell'iter dei documenti e fascicoli informatici	17
Comunicazione di cittadini e imprese con le amministrazioni pubbliche	18
Fruibilità dei servizi in rete e strumenti di accesso	19
Pagamenti elettronici	20
Il ruolo degli intermediari privati	20
IL CAMBIAMENTO NEL MODO DI OPERARE DELLA PUBBLICA AMMINISTRAZIONE	22
La gestione dei documenti informatici e dei flussi documentali	24
Gli adempimenti delle Amministrazioni	26
Gli strumenti per verificare l'identità dei cittadini	28
Gli adempimenti delle Amministrazioni	32
SPC: la pubblica amministrazione in rete	32
Gli adempimenti delle Amministrazioni	33
Il Riuso modulare del software	34
Gli adempimenti delle amministrazioni	35
La sicurezza dei dati e dei sistemi	36
Adempimenti delle Amministrazioni	37
La continuità operativa	38
Gli adempimenti delle Amministrazioni	39
Disponibilità dei dati pubblici	41
Gli adempimenti delle amministrazioni	43

Realizzazione e diffusione dei servizi in rete	43
Gli adempimenti delle amministrazioni	44
I pagamenti Elettronici	46
Gli adempimenti delle Amministrazioni	46
L'accompagnamento di DigitPA	48

APPENDICE A – DOCUMENTI DI APPROFONDIMENTO TECNICO: REGOLE TECNICHE E LINEE GUIDA

50

Regole tecniche per la formazione, tenuta e conservazione del documento informatico.	50
Regole tecniche per il protocollo informatico e per la gestione dei flussi documentali.	50
Linee guida per la generazione del contrassegno elettronico.	50
Delibera DigitPA sulle modalità per presentare la domanda di iscrizione nell'elenco pubblico dei prestatori di servizi di conservazione.	50
Linee guida per la vigilanza sui prestatori di servizi di conservazione.	51
DPCM di definizione delle caratteristiche delle firme elettroniche	51
Regole tecniche per la trasmissione di documenti attraverso la posta elettronica tra le pubbliche amministrazioni	51
DPCM su soluzioni alternative per le comunicazioni con ricevuta di invio e consegna	51
Regole tecniche per la realizzazione dei sistemi informativi unitari preposti alla gestione delle banche dati di interesse nazionale	51
Regolamenti per l'organizzazione del SPC	51
Linee guida per le convenzioni per l'utilizzo dei dati pubblici	51
DPCM di attuazione dell'art. 28, comma 3-bis	52
Regole tecniche per estrazione di elenchi di possessori di posta elettronica certificata	52
Regole tecniche per l'identificazione dell'autore di un'istanza presentata tramite PEC	52
Regole Tecniche per la sicurezza dei dati, dei sistemi e delle infrastrutture	52
Regole Tecniche per il riuso modulare del software	52
Linee guida sul riuso	52
Linee Guida sulla continuità operativa	53
Linee guida per le convenzioni di accesso ai dati delle amministrazioni	53
DM per la regolamentazione delle attività di pagamento	53
Regole tecniche per il trasferimento di fondi fra le amministrazioni	53

APPENDICE B – QUADRO DI CONFRONTO FRA I SISTEMI DI FIRMA ELETTRONICA PREVISTI NEL VECCHIO E NEL NUOVO ORDINAMENTO

54

RELAZIONE FRA VECCHIO E NUOVO SISTEMA DI FIRME

57

PREMESSA

Le nuove tecnologie dell'informatica e delle telecomunicazioni hanno profondamente modificato gran parte delle relazioni tra persone nel lavoro e nel tempo libero. Per cogliere questo fenomeno nello sviluppo già conseguito, ma anche nelle potenzialità di ulteriore dinamica basta pensare all'uso del telefono cellulare che, nato per la conversazione è ora uno strumento che consente di essere sempre e dovunque connessi in rete avendo a disposizione una quantità di servizi non solo di informazione, ma anche per più complesse transazioni. Tra i primi settori che hanno vista diffusa questa rivoluzione digitale sono stati per il grande pubblico quelli dell'informazione e dell'intrattenimento e per il mondo delle imprese, e più in generale dell'economia, le transazioni commerciali in tutti i loro aspetti.

Non ha avuto invece la veloce diffusione che ci si aspettava la digitalizzazione dei rapporti di cittadini e imprese con la Pubblica Amministrazione. Questo fenomeno non è soltanto italiano perché i livelli di digitalizzazione di questo settore sono abbastanza basti in generale nel mondo. Anzi proprio nell'ultimo biennio l'Italia ha raggiunto posizioni di eccellenza nella classifica europea di disponibilità dei servizi digitalizzati, come dimostrato dall'ultima indagine comparativa della Commissione Europea sullo stato di attuazione dei servizi di e-government nei 27 Paesi UE: "Digitizing Public Services in Europe 2010". La disponibilità online dei 20 servizi prioritari per cittadini ed imprese ha raggiunto il 100% (era il 69% nel 2009), contro una media europea dell'82%. La sofisticazione dei servizi offerti è ormai al livello più alto per la quasi totalità dei servizi prioritari. Insieme a Germania, Svezia e Portogallo è al 99% rispetto a una media EU27 di circa l'89%.

Le cause del ritardo non sono né la impreparazione tecnologica (la Pubblica Amministrazione italiana ha investito somme cospicue a questo scopo e dispone di sistemi informativi di buon livello), né la disattenzione del mondo politico (nel 2005 è stata adottata una legge ad hoc il cosiddetto Codice dell'Amministrazione Digitale strumento riconosciuto come all'avanguardia nel confronto internazionale).

Il Governo ha individuato i principali ostacoli che hanno limitato il successo:

- *la lentezza della Pubblica Amministrazione nel realizzare quelle innovazioni (nell'organizzazione, nelle procedure e nelle normative a carattere operativo) che erano indispensabili perché l'informatizzazione non fosse altro che rendere automatici i procedimenti in atto confermando le situazioni di irrazionalità e inefficienza presenti*

- *un diffusa prevenzione all'interno della Pubblica Amministrazione verso l'eliminazione del documento cartaceo anche per gli atti intermedi (il vecchio proverbio "carta canta" è duro da superare)*
- *la natura degli atti amministrativi che nel sistema italiano molto frammentato comporta l'intervento di più amministrazioni per cui spesso il cittadini deve curare anche il coordinamento dell'apporto di ciascuna di queste amministrazioni per avere il risultato atteso; questo fa sì che non basta informatizzare singoli segmenti, ma occorra invece garantire un'efficace prestazione del sistema nel suo complesso (assicurare cioè la cosiddetta interoperabilità dei sistemi informativi)*
- *la insufficiente attenzione alla fase conclusiva di effettiva erogazione del servizio agli utenti, per cui a fronte di elaborazioni dei dati ad alta tecnologia nei centri di calcolo della P.A. rimaneva la fila agli sportelli per avere informazioni ed ottenere servizi*
- *una scarsa attenzione a soluzioni di digitalizzazione concrete ed immediate (fra cui, ad esempio, l'invio di moduli e richieste all'amministrazione via posta elettronica certificata) rinviando l'attivazione del servizio all'utilizzo di soluzioni nuove più attraenti in teoria, ma in pratica inutilmente costose e comunque sempre in evoluzione e mai pienamente operative.*

In definitiva le azioni messe in atto dal Governo per superare le cause di questo ritardo sono state su due fronti: da una parte innovazione nei servizi messi a disposizione (migliore fruibilità dei servizi già offerti e offerta di nuovi servizi) dall'altra innovazione organizzativa e innovazione tecnologica nelle singole amministrazioni e nella loro capacità di interagire.

Usando la strategia di integrare funzionalità e servizi già realizzati da singole Amministrazioni, è possibile creare un circolo virtuoso capace di accrescere sensibilmente il potenziale innovativo del Paese: valorizzando e diffondendo progressivamente soluzioni di successo un numero sempre maggiore di persone avrà consapevolezza dei servizi via via realizzati, aumentando la richiesta di ulteriore innovazione.

I vantaggi per gli utenti sono concreti. Fra gli esempi:

- *non più code allo sportello, ma scambio di mail, sms e anche documenti via cellulare e Personal computer compresa la ricezione del documento conclusivo*
- *non più consegna ogni volta di copie documenti già in possesso della pubblica amministrazione*
- *non più inseguimento della pratica tra i vari uffici (sia dentro un'amministrazione, sia tra più amministrazioni), ma in rete tracciabilità piena e tempestiva dello stato di avanzamento di una pratica*

Numerosi e molto incisivi sulla qualità della vita e sull'efficienza quotidiana sono i settori ai quali si riferiscono queste nuove modalità di interazione: tra questi, la

giustizia, la scuola, la salute, la sicurezza sono certamente prioritari per il grande pubblico, ma di grande rilievo sono anche i settori che riguardano le attività produttive industria artigianato servizi.

Al di fuori della Pubblica Amministrazione servizi di questo tipo sono di uso comune da tempo: si pensi alla tracciabilità di una spedizione di plico via corriere, o al sistema di prenotazione e check-in per i viaggi aerei o alla gestione in rete dei conti correnti o al bancomat.

La riforma del Codice dell'Amministrazione Digitale, che sarà descritta nei capitoli seguenti, definisce azioni concrete, obblighi e scadenze perché si realizzi il quadro sopra delineato. Gli interventi sono di varia natura:

- *modifica integrazione e precisazione del quadro normativo per realizzare il pieno valore giuridico delle transazioni digitali (per esempio il valore della stampa su carta di un documento originato in forma digitale e la semplificazione e il rafforzamento dei meccanismi di riconoscimento in linea del soggetto che attiva una transazione digitale)*
- *standard e regole tecniche per assicurare la sicurezza e l'interoperabilità delle transazioni (i vari strumenti diventano un sistema integrato che consente varietà dei punti di accesso, molteplicità di dispositivi e risposte coordinate)*
- *scadenze cogenti per la messa a disposizione dei servizi con meccanismi di incentivi e disincentivi per i responsabili dell'eventuale mancato rispetto delle scadenze*
- *informazione agli utenti sui servizi disponibili (quale amministrazione presta quali servizi in linea e attraverso quali canali è contattabile, ma anche come l'utente può esprimere il proprio grado di soddisfazione per i servizi erogati)*
- *miglioramento dell'assistenza (a partire dai call center per avere notizie e risolvere questioni specifiche) senza presentarsi agli sportelli.*

Volendo riassumere in una parola, la riforma del CAD si può usare il termine "esigibilità" per sottolineare che il rapporto per via digitale tra cittadini e pubblica Amministrazione è un diritto concreto al quale va data attuazione: come tutti diritti ne vanno precisati i termini le modalità di fruizione e va sanzionato chi non adempie al corrispondente obbligo di metterlo a disposizione.

La semplificazione dei rapporti di cittadini e imprese con la Pubblica Amministrazione non è solo l'attuazione di diritti fondamentali, ma dispiega i suoi effetti sulla produttività del paese (tempi e costi) e quindi sulla competitività nello scenario internazionale, ma aumenta anche la trasparenza e conseguentemente la correttezza dell'azione amministrativa. Rilevante anche l'impatto positivo che la digitalizzazione della Pubblica Amministrazione genera sul grado di

consapevolezza e partecipazione dei cittadini, un'occasione per accelerare il cambiamento e per una crescita complessiva del Paese.

Il volumetto è rivolto sia al grande pubblico sia alle amministrazioni e vuole informare gli utenti e gli addetti ai lavori delle concrete possibilità che si stanno aprendo, sulle modalità per fruirne, sui canali disponibili per migliorare la fruizione, ma anche per una più generale opportunità di crescita complessiva anche in termini di integrazione e coesione tra le diverse componenti della società.

IL CAMBIAMENTO PER CITTADINI E IMPRESE

Il nuovo testo legislativo del Codice dell'Amministrazione Digitale rappresenta una spinta importante al cambiamento, non solo per i nuovi e numerosi elementi di innovazione che indica alle pubbliche amministrazioni, sul fronte del miglioramento dei servizi per cittadini e imprese ma anche perché introduce nuovi diritti e nuove opportunità valide nei rapporti fra privati. Lo spirito della riforma e le prospettive di cambiamento insite nell'applicazione dei dettami normativi tracciano un percorso innovativo di notevole portata e di sicuro impatto sui cittadini sia come soggetti fruitori dei servizi pubblici sia quando impegnati in rapporti con interlocutori privati.

Molte sono le novità che investono di nuovi diritti e opportunità cittadini e imprese e permettono loro di acquisire un nuovo ruolo: essi stessi sono protagonisti, motore dell'innovazione e traino al cambiamento. Il nuovo Codice stabilisce il principio secondo il quale gli utenti costituiscono il principale stimolo alla modernizzazione dei servizi attraverso l'uso delle tecnologie, trascinando le pubbliche amministrazioni che saranno così chiamate a rispondere alle più moderne richieste dei cittadini e delle imprese. Documento informatico, posta elettronica certificata, pagamenti elettronici, fruibilità dei dati e accesso semplificato ai servizi: sono alcuni dei pilastri che contribuiscono a favorire l'evoluzione di molti comportamenti dei cittadini, su cui si fonderà di conseguenza l'efficientamento e l'aumentata efficacia delle risposte delle PA.

L'impatto dell'innovazione non va cercato solo nei vantaggi conseguenti all'utilizzo di nuove modalità e strumenti, ma anche e soprattutto negli elementi di cambiamento *tecnologico, organizzativo e procedurale* del rapporto tra amministrazione e cittadini e imprese e del rapporto fra privati. Una pubblica amministrazione più vicina alle esigenze del cittadino, più trasparente, diventa un soggetto affidabile, in un processo di crescita di fiducia in grado di generare benefici in tutto il sistema-paese, andando a colmare il gap di affidabilità e di immagine che ancora oggi è presente nei rapporti tra pubbliche amministrazioni e cittadini.

La prima parte del capitolo – Elementi generali dell'innovazione digitale - descrive gli elementi innovativi del Codice validi in qualunque contesto e i principi chiave dell'agire digitale nel rapporto tra privati e tra questi e le amministrazioni. Pertanto, si sofferma principalmente sulle innovazioni introdotte in riferimento al documento informatico, la sua validità, conservazione e trasmissione e sul tema dell'identità digitale.

La seconda parte del capitolo – L'innovazione digitale nel rapporto con l'amministrazione - approfondisce le novità per i cittadini e le imprese in merito ai canali e agli strumenti utilizzabili specificamente nei rapporti con l'amministrazione: canali e strumenti che favoriscono la comunicazione e i procedimenti tra imprese e PA, e tra cittadini e PA, le possibilità offerte dalla tecnologia per accelerare i tempi di erogazione dei servizi e per accrescere la soddisfazione dell'utente.

Elementi generali dell'innovazione digitale

I nuovi scenari e le nuove opportunità indicate dal Codice introducono interessanti novità in termini di diritti per i cittadini e le imprese in un ambito più esteso di quello del rapporto con l'amministrazione. La riforma digitale che da oggi si avvia introduce un cambiamento a favore dei fruitori dei servizi della PA in un processo concreto di miglioramento della qualità e dell'efficienza amministrativa che ha effetti anche nel rapporto fra soggetti privati, diritti che i cittadini possono far valere in molteplici ambiti della *vita di tutti i giorni*: nei rapporti con il mondo bancario ed assicurativo, con i professionisti, con le imprese di servizi, con i datori di lavoro privati...

Documenti informatici e loro validità

La carta è costosa, preziosa e alla lunga ingombrante. Molto spesso, per esibire un documento cartaceo, qualcuno stampa su carta dei dati che sono stati creati e memorizzati in formato digitale. Addirittura può capitare che chi richiede e poi riceve il documento su carta lo passi in uno scanner per memorizzarlo di nuovo su un PC.

Da oggi in poi i cittadini possono evitare, se lo desiderano, il passaggio “dal PC alla carta”. Infatti, i documenti in formato digitale, i cosiddetti *documenti informatici*, sono validi e possono sostituire, sempre e per qualsiasi utilizzo, i classici documenti di carta, chiamati dal Codice *documenti analogici*.

Per eliminare ogni dubbio riguardo alla possibilità di usare un documento informatico al posto del *pezzo di carta* e per rafforzare la certezza dei cittadini rispetto all'esigibilità di questo nuovo diritto, il Codice dà molto spazio alla definizione di cosa siano il documento informatico, le diverse tipologie delle sue copie e le condizioni di validità giuridica.

Infatti, il Codice assegna, come direbbero i giuristi, al documento informatico valore probatorio, liberamente valutabile in giudizio: un dettato normativo fondamentale per favorire il passaggio definitivo dalla carta al digitale sia nel rapporto con l'amministrazione sia nei rapporti fra privati.

Più nel dettaglio, il documento informatico, è definito come una “rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”, ovvero una sequenza di bit che mantiene la sua validità indipendentemente dal supporto utilizzato (CD, DVD, pen-drive...).

E' interessante approfondire il significato che il Codice assegna al concetto di copia¹ e di duplicato² e come ne disciplina la validità e l'utilizzo nel contesto del documento informatico. Vediamo quindi le definizioni e le diverse applicazioni di questi concetti che probabilmente sono noti nel tradizionale ambito delle copie cartacee e dei duplicati cartacei, ma che il mondo digitale mette in una nuova prospettiva:

- *copia informatica di un documento (cartaceo) analogico*: si tratta di un file che ha lo stesso contenuto del documento analogico (cartaceo nella maggior parte dei casi) di cui è la copia, ma che può essere elaborato, ad esempio da un programma che lo

¹ Riproduzione di un documento originale

² Riproduzione di un documento originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali

“legge” , lo registra in memoria e magari lo presenta in un formato diverso da quello originario, pur conservando intatto il contenuto. Quindi: identico contenuto, diverso formato, originale cartaceo e copia in digitale.

- *copia per immagine su supporto informatico di un documento analogico*: è un documento informatico identico per contenuto e forma all'originale, ad esempio un file immagine (in formato: .jpeg, .gif, .tiff, ...) ottenuto dalla scansione del documento cartaceo, che non permette di modificare né il contenuto né la forma dell'originale. Quindi: identico contenuto, identico formato, originale in cartaceo e copia in digitale.
- *copia informatica di documento informatico*: in questo caso si fa riferimento a un file con contenuto identico all'originale ma diverso formato digitale, ad esempio il documento informatico originario è un file di testo .txt o .doc mentre la copia è la versione .pdf del documento stesso. Quindi: identico contenuto, diverso formato, originale e copia in digitale.
- *duplicato informatico*: è un file che, avendo la stessa sequenza binaria, è uguale in tutto e per tutto all'originale, è la stessa sequenza di bit. In pratica, il risultato che chiunque può ottenere facendo il “copia e incolla” di un file da una cartella ad un'altra o da un computer a una chiavetta usb o hard disk esterno. Quindi: identico contenuto, identico formato, originale e copia in digitale.

Per quanto riguarda la validità delle copie informatiche di documenti analogici, il Codice è chiaro: “qualunque documento informatico contenente copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico”, ha piena validità giuridica se viene rilasciato o spedito da un depositario pubblico autorizzato o da un pubblico ufficiale che vi appone la propria firma digitale.

La “copia per immagine” di un documento analogico ha valore probatorio se un notaio o un altro pubblico ufficiale ne attesta la conformità attraverso una dichiarazione allegata alla copia informatica.

Infine, i duplicati e le copie informatiche di documenti informatici (se prodotti secondo le regole definite dal Codice) hanno valore giuridico, se la loro conformità all'originale è attestata da un pubblico ufficiale.

Il Codice non dimentica che non tutti i processi fra privati e fra cittadini e imprese ed amministrazione sono pronti da subito ad abbandonare la carta.

Quante volte viene ancora chiesto al cittadino, per “aprire una pratica” – con la banca, con l'Avvocato, per iscrivere i figli a scuola, per stipulare un'assicurazione, con un professionista, per fare un passaggio di proprietà in un'agenzia di servizi - di portare o di spedire dei documenti cartacei, magari in fotocopia firmata? Ma i ritardi di alcuni non devono rallentare tutti: meglio una digitalizzazione graduale e parziale che nessuna digitalizzazione oggi con la speranza di una digitalizzazione completa domani...

Ebbene, il Codice prevede che i documenti, a seconda del livello di informatizzazione e di innovazione disponibili, possano *appoggiarsi* al digitale per una parte, la più

tecnologicamente pronta, del processo e passare alla carta quando il cittadino si trovi di fronte ad interlocutori ancora non aggiornati, il tutto non perdendo la validità e il valore probatorio del documento originale. Questo è possibile con l'introduzione del *contrassegno digitale*, che consiste nel riprodurre sulla carta una sorta di firma, di impronta unica ed univoca del documento informatico originario, che dà la garanzia che la copia su carta è identica all'originale informatico e non c'è stata alcuna contraffazione.

Quindi un documento informatico (ad esempio un certificato di residenza) munito di contrassegno digitale e inviato con modalità telematiche al cittadino da un'amministrazione virtuosa, può essere utilizzato in formato digitale, se gli interlocutori sono parimenti virtuosi, oppure stampato ed esibito in formato cartaceo, con il contrassegno a garantirne la validità e la conformità all'originale.

Infine, per quanto riguarda la validità dei documenti amministrativi informatici, quindi documenti rilasciati da un'amministrazione pubblica in formato, il Codice stabilisce che:

- se prodotti attraverso strumenti informatici, possono essere duplicati e copiati su diversi o identici tipi di supporto per gli usi consentiti dalla legge;
- se sono copie su supporto informatico di documenti analogici, hanno la stessa validità probatoria dell'originale se sono autenticati attraverso firma digitale da un funzionario delegato dall'Amministrazione;
- se copiati su supporto analogico, la loro validità è assicurata dall'apposizione di un contrassegno digitale.

Conservazione digitale dei documenti

Conservare correttamente ed efficacemente i documenti negli anni, per poi poterli trovare ed esibire a distanza di tempo è un aspetto fondamentale sia per le amministrazioni pubbliche e per i soggetti anche privati che si trovano a gestire milioni di documenti sia per i singoli cittadini che sono tenuti a conservare, per alcuni anni, ricevute, attestazioni, contratti, dichiarazioni: chi non ha messo a soqquadro la propria casa temendo di aver perso la ricevuta del pagamento di una rata del mutuo, acceso anni prima, o di una multa già pagata da tempo, o il contratto di compravendita di una casa, magari ricevuta in eredità?

Su questo aspetto, il Codice dell'Amministrazione Digitale definisce un principio importante: tutti i documenti che per legge o regolamento devono essere conservati – documenti degli archivi, scritture contabili, corrispondenza, anche fra privati – possono essere riprodotti e conservati su supporto informatico e sono validi a tutti gli effetti di legge. La loro riproduzione e relativa conservazione devono essere effettuate in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo. In caso di documenti prodotti originariamente in modalità informatica, è obbligatorio che la loro conservazione permanente avvenga con modalità digitali. Questo vuol dire, per il cittadino, avere molta più facilità sia nel conservare sia nel richiedere, in formato digitale, documenti che devono essere conservati nel tempo anche nel caso di atti che una pubblica amministrazione possiede nel proprio archivio. Vuol dire anche mettere un freno alla proliferazione degli archivi cartacei, costosi e difficili da gestire sia per le amministrazioni

sia per i privati – si pensi solo agli spazi necessari a conservare milioni di documenti di carta - e carenti dal punto di vista della sicurezza e dell'integrità della conservazione.

Il Codice disciplina in maniera molto precisa quali debbano essere i requisiti di un sistema per la conservazione dei documenti informatici, che per essere a norma deve assicurare, fra l'altro, l'integrità dei documenti conservati e la loro facile ed agevole reperibilità e fruizione, oltre all'identificazione certa del soggetto e dell'amministrazione ha formato i documenti.

Una novità importante riguarda la possibilità, per le amministrazioni, di avvalersi di soggetti, pubblici o privati appositamente accreditati e dotati di requisiti verificati dal punto di vista della qualità, della sicurezza, dell'organizzazione e delle capacità tecnologiche, che possono coadiuvarle nella gestione del sistema di conservazione, in termini di:

- gestione completa del sistema di conservazione dei documenti informatici,;
- certificazione della conformità del processo di conservazione gestito in proprio dall'amministrazione.

Identità digitale e trasmissione digitale dei documenti

L'identità digitale, ovvero l'identificazione univoca di un soggetto per via telematica, è un prerequisito decisivo per dispiegare efficacemente il processo di erogazione on line di molti servizi pubblici e, in generale, per consentire una piena comunicazione in via telematica fra cittadino e amministrazioni. Infatti, per poter effettuare transazioni in rete (pagamenti, acquisti, richiesta di servizi, accesso a dati riservati) con assoluta sicurezza ed affidabilità, è necessario avere la certezza, ottenibile attraverso particolari requisiti tecnologici di sicurezza, che ad un utenza digitale (cioè, ad esempio, ad un *nomeutente* e ad una *password*) sia associato univocamente un soggetto fisico o giuridico, sia esso cittadino o azienda.

Le ultime modifiche apportate al Codice dell'Amministrazione Digitale definiscono con chiarezza quali sono gli strumenti e le modalità di identificazione attraverso i quali poter usufruire di servizi on line e presentare istanze e dichiarazioni a una pubblica amministrazione.

Essi sono:

- la firma digitale;
- la Carta d'Identità Elettronica, ovvero il documento di identità rilasciato ai cittadini dai Comuni, provvisto di banda magnetica e microchip, e la Carta Nazionale dei Servizi, strumento di accesso ai servizi on line rilasciata a discrezione delle singole Amministrazioni;

- la casella di posta elettronica certificata (PEC), in cui le credenziali di accesso sono rilasciate previa identificazione, anche telematica, del titolare della casella;
- altri strumenti che consentono l'individuazione del soggetto che richiede il servizio, compreso l'invio per via telematica delle istanze e la copia fotostatica del documento di identità.

In particolare, l'utilizzo della PEC rappresenta una modalità di identificazione che facilita e amplia molto le possibilità di interazione on line a disposizione del cittadino, soprattutto se considerata insieme alla possibilità per i cittadini di ottenere gratuitamente questo strumento iscrivendosi al servizio "PostaCertificat@" (www.postacertificata.gov.it). Attraverso la propria casella PEC, infatti, sarà possibile inviare a qualunque Amministrazione istanze e dichiarazioni valide a tutti gli effetti di legge, senza la necessità di dover produrre altra documentazione che accerti la propria identità.

Questa possibilità è coerente con l'impostazione generale del nuovo Codice dell'Amministrazione Digitale, dove il campo di utilizzo della PEC viene reso ancora più esteso per i cittadini e le imprese e vincolante per le Amministrazioni. L'invio di documenti tramite PEC è equivalente alla notificazione per mezzo della posta tradizionale "salvo che la legge disponga diversamente": quindi l'invio di documenti ed istanze alla PA tramite posta elettronica certificata va sempre bene, a meno che non sia esplicitamente proibito. Il cittadino non deve più domandarsi: "La posso usare?" ma è l'amministrazione che deve chiaramente indicare i casi in cui non sia possibile usare la PEC.

Quindi, le amministrazioni:

- devono utilizzare la posta certificata per tutte le comunicazioni che necessitano di una ricevuta di invio e di una di consegna – ciò che finora veniva fatto con la raccomandata A/R – verso cittadini che hanno preventivamente comunicato il proprio indirizzo di PEC;
- devono pubblicare i propri indirizzi di posta elettronica certificata nell'Indice delle Pubbliche amministrazioni, che costituisce la rubrica degli indirizzi delle amministrazioni, accessibile e consultabile da tutti all'indirizzo www.indicepa.gov.it;

mentre i cittadini:

- accettano automaticamente l'invio di atti e provvedimenti che li riguardano da parte delle pubbliche amministrazioni una volta dichiarato il proprio indirizzo PEC
- possono trovare gli indirizzi di PEC dei diversi enti all'indirizzo: www.indicepa.gov.it.

Per il cittadino l'utilizzo della PEC costituisce un'opportunità importante, non solo in termini di velocità e certezza della trasmissione e dell'invio – si pensi alla diminuzione dei rischi di smarrimento della corrispondenza - ma anche perché diventerà molto più semplice conservare e ricercare nel tempo le comunicazioni con le pubbliche amministrazioni: ogni cittadino dotato di PEC si potrà creare una sorta di fascicolo

personale delle comunicazioni con la PA, semplicemente archiviando sul proprio PC i messaggi di posta certificata.

Se per i cittadini la comunicazione telematica con le amministrazioni è un'opportunità, per le imprese è un obbligo: come normato dal Codice, infatti, la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni tra imprese e pubbliche amministrazioni avviene esclusivamente utilizzando modalità telematiche, in coerenza con l'obbligo, per tutti i professionisti iscritti ad albi professionali, di possedere un indirizzo di posta elettronica certificata.

L'innovazione digitale nei rapporti con l'amministrazione

L'innovazione digitale racchiusa nel nuovo Codice, in virtù dei molti e diversi cambiamenti di cui pone le basi, appare di grande interesse per la nuova dimensione dei rapporti tra cittadini, imprese e pubbliche amministrazioni, spinta decisiva verso l'effettiva realizzazione dell'amministrazione digitale.

Nei prossimi paragrafi è proprio questa innovazione al centro dell'attenzione: un cambiamento di modalità, strumenti e un insieme di diritti e doveri, che cambia la cultura e forse segna il passaggio cruciale verso una nuova realtà, una società dell'informazione della conoscenza aperta a tutti.

I cittadini e le imprese hanno diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione pubblica. Non sarà più possibile quindi per un ente o per un gestore di pubblico servizio obbligare i cittadini ad andare *allo sportello* per presentare documenti cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti: per tutto questo deve essere sempre e dovunque disponibile un canale digitale (che, nella maggior parte dei casi, può essere rappresentato dalla PEC) sicuro, certificato e con piena validità giuridica che permetta di dialogare con l'amministrazione da un computer. Il digitale diventa la regola nei rapporti tra imprese ed amministrazioni e il cartaceo l'eccezione: gli enti dovranno utilizzare le comunicazioni cartacee solo quando sia impossibile utilizzare quelle telematiche e dovranno consentire a cittadini ed imprese di inoltrare istanze e di effettuare pagamenti per via telematica.

La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le stesse modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.

La posta Elettronica Certificata diventa, per tutte le imprese e i professionisti, che per legge devono esserne dotati, e per i cittadini che lo desiderano il mezzo più veloce, sicuro e valido per comunicare con le amministrazioni pubbliche. Da lì passano comunicazioni, atti e provvedimenti, ma anche istanze e dichiarazioni che un cittadino può trasmettere usando la propria casella PEC anche come strumento di identificazione che può evitare, nella maggior parte dei casi, l'uso della firma digitale. È prevista poi una più ampia possibilità di accesso ai servizi che si basa sia sulla Carta d'Identità elettronica e carta dei servizi sia su altri strumenti che comunque consentano l'individuazione del soggetto che richiede il servizio.

Le amministrazioni dovranno curare maggiormente i contenuti dei propri siti web, che diventano sempre più il vero front-office nei confronti dei cittadini e delle imprese, in cui si dà conto dei servizi online a disposizione degli utenti e sono pubblicate dettagliate informazioni di contatto, di trasparenza e di operatività dell'azione amministrativa. Le PA devono condividere, diffondere e riutilizzare i dati pubblici di cui sono titolari: ai cittadini non devono essere richiesti dati e informazioni già in possesso dell'amministrazione.

Il percorso di riforma potrà essere costantemente verificato e valutato proprio da coloro che sono i beneficiari della riforma stessa: le amministrazioni devono rendere disponibili

strumenti per la valutazione dei dirigenti e delle organizzazioni, consentendo di fatto al cittadino di essere concretamente partecipe al miglioramento della qualità dei servizi. La corretta attuazione delle indicazioni del Codice sarà quindi monitorata anche grazie alla costante ed obbligatoria misurazione del livello di soddisfazione degli utenti, di cui le amministrazioni sono tenute a tener conto adottando strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti quando usufruiscono di un servizio on line.

Il nuovo Codice introduce pertanto un insieme di innovazioni normative che vanno a incidere concretamente sui comportamenti e sulle prassi delle amministrazioni e sulla qualità dei servizi resi. La riforma rende effettivi i diritti per cittadini e imprese e cogenti gli obblighi per la PA.

Un cambiamento che semplifica e migliora il rapporto con l'amministrazione, trasformandolo in un rapporto diretto e di interazione paritaria tra le parti. Il cittadino, abituato di frequente ad essere parte "passiva" di un procedimento amministrativo, di cui subisce ritardi, inadempienze, senza avere, spesso, la contezza di ciò che accade e del perché accade, è destinato a diventare completamente partecipe e informato, in condizione di valutare i servizi e di interagire secondo una più stretta e corretta relazione cliente/fornitore.

Contenuto dei siti pubblici: informazione e trasparenza

Le Pubbliche Amministrazioni sono tenute ad aggiornare i dati e le notizie che per legge devono essere pubblicati sul proprio sito istituzionale:

- l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio di livello dirigenziale non generale, i nomi dei dirigenti responsabili dei singoli uffici, il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, con documenti anche normativi di riferimento;
- l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale;
- le scadenze e le modalità di adempimento dei procedimenti;
- l'elenco completo delle caselle di posta elettronica e posta elettronica certificata istituzionali attive;
- le pubblicazioni, i messaggi di informazione e di comunicazione;
- l'elenco di tutti i bandi di gara;
- il testo integrale dei bandi di concorso;
- l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando, in quest'ultimo caso, i tempi previsti per l'attivazione.

In questo obbligo rientra anche quello di pubblicare online l'elenco dei documenti richiesti al cittadino per avviare un procedimento (moduli e formulari). Le amministrazioni non

potranno più richiedere al cittadino di utilizzare moduli o formulari che non siano stati pubblicati sul web; in caso di mancata pubblicazione, inadempienza rilevante ai fini della misurazione e valutazione della performance dei dirigenti responsabili, i cittadini potranno avviare il procedimento senza presentare alcun modulo.

Il cittadino (sia privato che imprenditore) acquisisce diritti sempre più ampi all'informazione e alla trasparenza dell'operato della PA, attraverso le tecnologie con la semplice consultazione dei siti web delle pubbliche amministrazioni, avrà a disposizione tutte le informazioni di cui ha bisogno. Il Codice rafforza infatti il percorso già avviato dalla Riforma Brunetta - D.Lgs 150/09 - in termini di trasparenza delle amministrazioni pubbliche, percorso che vede necessariamente nei siti internet pubblici uno dei principali strumenti di pubblicità. Le amministrazioni devono tenere aggiornati i dati e le informazioni presenti sui siti web e devono trasmetterne una parte rilevante alla Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica che potrà così avere una conoscenza diretta di molti fenomeni, a partire ad es. dalla consistenza dei servizi online presenti, per poter avviare un confronto virtuoso fra le amministrazioni.

L'applicazione delle nuove indicazioni del Cad in materia di "contenuto dei siti pubblici" permetterà al cittadino/imprese di:

- "sapere a chi rivolgersi" all'interno di un'amministrazione, individuando precisamente la struttura organizzativa dell'amministrazione (organigramma, uffici, dirigenti e responsabili, ecc.), i procedimenti e le istruttorie
- "sapere come e a chi comunicare" attraverso l'elenco degli indirizzi di posta elettronica certificata attivi
- essere a conoscenza in tempo reale delle opportunità di impiego e di collaborazione nel settore pubblico, consultando i bandi di gara e i concorsi dell'amministrazione
- informarsi sui modi e tempi di erogazione dei servizi in rete
- utilizzare i servizi in via telematica per la soddisfazione delle proprie richieste amministrative, e verificarne a distanza lo stato di avanzamento
- fruire liberamente (in modo gratuito) dei dati pubblici senza necessità di identificazione
- utilizzare in via esclusiva documentazione (moduli e formulari) standard per le richieste di istanze alle Pa, evitando la possibilità di rigetto o di rimando per mancanza della modulistica

Certo, per i cittadini non è facile districarsi fra i tanti siti dell'amministrazione e arrivare rapidamente al servizio desiderato: per questo motivo le strutture del Ministro per la pubblica amministrazione e l'innovazione mettono a disposizione dei cittadini, già da subito, degli strumenti di aiuto alla navigazione nell'amministrazione digitale:

- www.italia.gov.it, il motore dell'amministrazione digitale, una sorta di rubrica della PA digitale, che focalizza la propria azione sull'essere il motore di ricerca della Pubblica Amministrazione, con un'organizzazione semplice per funzioni attivabili dal cittadino, al fine di conoscere *chi fa cosa, dove e come* nella PA;
- ViviFacile (www.vivifacile.gov.it) e Linea Amica (www.lineaamica.gov.it), servizi che, tramite fonia, sms e il contatto con operatori umani, sviluppano e forniscono tutta l'informazione e i servizi diretti al cittadino, valorizzando l'azione di assistenza e contatto diretto con gli utenti.

Tutti questi strumenti sono fra loro integrati per presentare al cittadino tutte le informazioni e o servizi esistenti nelle amministrazioni che, sempre più numerose, mettono a disposizione servizi attraverso i propri siti web.

Tracciabilità dell'iter dei documenti e fascicoli informatici

Si è già detto che il Codice conferma e rafforza la spinta verso la formazione, gestione e conservazione dei documenti informatici, dando alle amministrazioni forti indicazioni nella direzione di una sempre maggiore digitalizzazione e dematerializzazione documentale che favorisce un graduale “abbandono” della carta.

Per rafforzare la fiducia dei cittadini circa la validità dell'invio telematico di dati e documenti e per dare una pari dignità di trattamento amministrativo a tutte le comunicazioni, in qualunque modo pervenute all'amministrazione, il Codice stabilisce che ogni comunicazione inviata tramite PEC tra le Pubbliche Amministrazioni e tra queste e i cittadini o le imprese debba essere protocollata in via informatica. L'amministrazione titolare del procedimento raccoglierà gli atti, i documenti e i dati di uno stesso procedimento in un fascicolo elettronico, identificato in modo univoco e quindi in ogni momento identificabile senza difficoltà.

In questo modo si assicura la tracciabilità del documento, dell'intero procedimento amministrativo e del processo stesso di conservazione e archiviazione delle pratiche da parte della PA. E ovviamente si riducono sensibilmente i costi in termini economici, di tempo e risorse dedicate dall'amministrazione alla gestione dei fascicoli e degli archivi.

Inoltre, l'obbligo disposto genererà notevoli vantaggi a beneficio dei cittadini e delle imprese, fruitori dei servizi della pubblica amministrazione. Essi potranno, con maggiori garanzie, verificare la corretta acquisizione delle proprie richieste e delle proprie istanze, e potranno più facilmente far valere i propri diritti. Ridurre in modo significativo gli errori, identificando correttamente i documenti e le pratiche amministrative, riuscire a tracciare con sicurezza e velocità lo stato di una richiesta, ripercorrere la “storia” di ogni procedimento, non potranno che portare ad un miglioramento dello standard dei servizi resi. E ancora, una più facile condivisione delle informazioni, raccolte in un fascicolo elettronico, genera all'interno della amministrazione un meccanismo di trasferibilità di conoscenze utile all'intero sistema.

Questo cambiamento contribuirà a semplificare e facilitare i rapporti tra cittadini e imprese e pubbliche amministrazioni in quanto saranno meno onerose e più trasparenti le interazioni, la capacità di risposta e di gestione della pratica sarà più efficiente e trasparente, mentre, in parallelo, gli spostamenti fisici e la necessità di recarsi agli sportelli saranno ridotti al minimo. Sarà favorita la concorrenza positiva fra amministrazioni e i cittadini avranno un interlocutore autorevole con cui dialogare “parlando” la lingua delle moderne tecnologie.

Comunicazione di cittadini e imprese con le amministrazioni pubbliche

Il nuovo Codice dà impulso al processo di innovazione semplificando anche i flussi di informazione/comunicazione tra cittadini/imprese e amministrazioni pubbliche.

Per le imprese viene introdotto un concetto e un modello di comunicazione che supera il tradizionale e, spesso, farraginoso iter di scambio di informazioni: la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, tra le imprese e le pubbliche amministrazioni avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le stesse modalità le amministrazioni pubbliche comunicano atti e provvedimenti amministrativi alle imprese. Qui l'impatto dell'innovazione è molto forte: il Codice sancisce un obbligo per le pubbliche amministrazioni e per gli operatori del mercato che scambiano dati con esse, ad utilizzare le tecnologie della comunicazione e dell'informazione. Obbligo che fino ad oggi non c'era e che da domani permetterà di avere una PA più informatizzata e meno burocratizzata nei suoi rapporti con il mondo delle imprese.

Rendere più facile l'accesso ai dati e attuare una comunicazione a due vie mediante strumenti telematici, orienta i servizi verso un livello di qualità più elevato e standardizzato, colmando le differenze di velocità tra privato e pubblico, anche rispetto ai concetti di efficienza, efficacia e trasparenza.

Il passaggio all'esclusività dell'utilizzo di tecnologie, nei rapporti fra PA ed imprese, sicuramente porterà ad un'accelerazione significativa della diffusione di innovazione tecnologica anche nel settore privato, con benefici di competitività anche rispetto ad un contesto internazionale dove l'impresa deve essere sempre più veloce a recepire e utilizzare l'innovazione tecnologica.

Per tutti, l'utilizzo della posta elettronica certificata è ampliato: le amministrazioni pubbliche utilizzano la PEC per le comunicazioni con tutti i soggetti che hanno preventivamente dichiarato il proprio indirizzo. La dichiarazione dell'indirizzo vincola solo colui che lo dichiara e rappresenta espressa accettazione dell'invio, tramite PEC, da parte delle pubbliche amministrazioni degli atti e dei provvedimenti che lo riguardano. Ogni istanza o dichiarazione si può presentare all'amministrazione per via telematica, mediante la propria casella di posta elettronica certificata, purché credenziali di accesso – nome-utente e password - siano state rilasciate solo dopo la verifica dell'identità del richiedente.

La PEC diventa il mezzo più veloce, sicuro e valido per comunicare con le PA. I cittadini possono utilizzare la PEC anche come strumento di identificazione, in molti casi evitando l'uso della firma digitale. Infatti, vengono limitati i casi in cui è richiesta la sottoscrizione dei documenti mediante firma digitale e sono previsti strumenti di firma più semplici, senza pregiudizio di sicurezza e attendibilità.

Riassumendo, il nuovo Cad sul tema delle modalità di comunicazione con la PA, offre a cittadini e imprese nuove opportunità e diritti, che si basano sull'applicazione del concetto di far viaggiare le informazioni e non le persone, come:

- diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione pubblica. Non sarà più possibile quindi per un'amministrazione obbligare i cittadini/imprese a recarsi agli sportelli per presentare documenti

cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti: per tutto questo deve essere sempre e dovunque disponibile un canale digitale sicuro, certificato e con piena validità giuridica che permetta di dialogare con la PA dal proprio computer.

- tutte le comunicazioni effettuate attraverso la posta elettronica certificata o attraverso altre soluzioni tecnologiche che via via saranno individuate, equivalgono alla notifica per mezzo della posta.
- attraverso la PEC passano comunicazioni, atti e provvedimenti, ma anche istanze e dichiarazioni che un cittadino può trasmettere, usando la propria casella di posta certificata anche come strumento di identificazione che può evitare, nella maggior parte dei casi, l'uso della firma digitale.

Fruibilità dei servizi in rete e strumenti di accesso

Le amministrazioni devono valorizzare e rendere fruibili i dati da esse posseduti (*i dati pubblici*). Il Codice favorisce la circolazione e l'accesso ai dati pubblici, affidando alla responsabilità delle amministrazioni aggiornare, divulgare e permettere la valorizzazione di essi, sfruttando in particolare la pubblicazione sul proprio sito istituzionale con modalità e formati "aperti", che non richiedano quindi all'utente di installare sul proprio PC software con licenze proprietarie. Infatti, l'accesso ai dati pubblici è gratuito e la pubblicazione dei dati in formato aperto ne deve permettere la rielaborazione da parte di terze parti.

Sempre secondo il principio di far viaggiare i dati e non le persone, le amministrazioni devono condividere, nel rispetto della privacy dei cittadini, i dati di cui sono titolari: un'informazione data una volta ad un'amministrazione o di proprietà dell'amministrazione stessa non deve più essere richiesta al cittadino, ma deve essere messa a disposizione delle altre PA interessate.

Il nuovo Codice afferma la centralità della corretta gestione del patrimonio informativo pubblico, e ripropone la definizione di "basi di dati di interesse nazionale" - che costituiscono un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali che deve garantire l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. Innovativa rispetto al passato l'indicazione di quali sono le basi di dati di interesse nazionale, e precisamente:

- a) repertorio nazionale dei dati territoriali;
- b) indice nazionale delle anagrafi;
- c) banca dati nazionale dei contratti pubblici;
- d) casellario giudiziale;
- e) registro delle imprese;
- f) gli archivi automatizzati in materia di immigrazione e di asilo.

Pagamenti elettronici

I pagamenti verso le PA possono essere effettuati con strumenti informatici. Il Codice stabilisce infatti che le pubbliche amministrazioni consentono il pagamento delle somme ad esse spettanti e a qualsiasi titolo dovute con l'uso delle tecnologie dell'informazione e della comunicazione.

Una novità importante è la definizione del “come” effettuare i pagamenti: il nuovo CAD introduce infatti alcuni strumenti operativi e di largo uso (carte di credito, di debito o prepagate e ogni altro strumento di pagamento elettronico disponibile, come ad esempio la scheda prepagata del cellulare) per consentire alle Pubbliche Amministrazioni di riscuotere i pagamenti. Inoltre, permette loro di avvalersi di soggetti anche privati per la riscossione aprendo di fatto un nuovo mercato dei servizi.

Nella costruzione dell'amministrazione digitale, che sfrutti in tutte le sue caratteristiche i vantaggi della tecnologia, l'impulso dato da questa innovazione normativa, è sicuramente di rilevante importanza e avvicina il modo di rapportarsi dei cittadini alla PA a normali comportamenti diventati di largo e uso quotidiano e di normale e diffuso utilizzo nell'accesso a servizi on-line (home banking, aste on-line, acquisti in rete).

Permettere l'uso della carte di credito, del bancomat, del cellulare e di altri strumenti di pagamento entrati nella pratica quotidiana della maggior parte dei cittadini sarà un ulteriore elemento di semplificazione e di avvicinamento fra cittadini e amministrazione: la PA prende atto degli strumenti tecnologici già conosciuti e diffusi fra i cittadini e si rende disponibile ad integrarli nei propri processi di *sportello telematico*.

Pagare elettronicamente l'amministrazione al vantaggio di evitare gli spostamenti e diminuire i tempi, affianca l'opportunità di creare un'immagine dell'amministrazione e un clima di rapporti PA/cittadino più amichevole e volto alla collaborazione ed alla apertura nei confronti della collettività. Se fino a ieri, il pagamento verso l'amministrazione - di per sé non certo un “piacere” per il cittadino! - risultava spesso complicato e lontano da una pratica quotidiana in cui il passaggio di denaro contante è oramai ridotto al minimo, d'ora in poi anche da questa azione potrà derivare semplificazione e maggiore attenzione verso i cittadini.

Il ruolo degli intermediari privati

Per facilitare ulteriormente l'utilizzo dei servizi digitali da parte di cittadini e imprese e per accelerare il dispiegamento dell'innovazione nelle amministrazioni, le PA può ricorrere a soggetti privati per lo svolgimento di alcune funzioni, ottenendo, anche sulla base di un'attenta analisi costi-benefici, risparmi di tempo (il servizio innovativo è erogato da chi già lo sa fare) e di denaro (l'amministrazione non deve acquisire funzioni e competenze che non le appartengono). Si aprono quindi per il mondo dell'impresa privata nuovi mercati di servizi che potranno contare su migliaia di clienti diretti (le amministrazioni) e milioni di clienti indiretti (i cittadini).

Oltre ad essere sancito come principio generale valido quindi per qualsiasi tipologia di servizio offerto in modalità telematica, il ricorso a intermediari privati è esplicitamente indicato alla PA in due casi:

- nell'effettuazione di pagamenti con modalità informatiche;
- nello svolgimento di attività di conservazione dei documenti informatici

Per il cittadino, il primo caso è sicuramente quello con un impatto più diretto. D'ora in avanti, infatti, per consentire i pagamenti telematici di quanto dovuto (per tasse, imposte, costi di erogazione di servizi, spese di segreteria...) le amministrazioni che devono mettere a disposizione dei servizi ad hoc potranno affidarsi a prestatori privati di servizi di pagamento. Un bel vantaggio per l'utente, che potrà accedere ai servizi pubblici più avanzati mediante modalità di pagamento che già utilizza e conosce alla perfezione, evitando di recarsi di persona allo sportello per concludere la transazione.

Nel caso della conservazione dei documenti informatici, invece, la possibilità del ricorso ad intermediari privati si riferisce all'attività interna alle Amministrazioni di gestione dell'archivio documentale. In questo processo, che fino ieri doveva essere gestito esclusivamente all'interno dell'ente, d'ora in poi i privati, selezionati sulla base di specifici requisiti, potranno affiancare le Amministrazioni che lo ritengono opportuno, in due diverse modalità di supporto:

1. la totale gestione del processo di conservazione dei documenti informatici, che può quindi essere affidato *in toto* all'esterno, a soggetti accreditati che garantiscano adeguate garanzie dal punto di vista organizzativo, tecnologico e di sicurezza;
2. la certificazione della conformità del processo di conservazione alle regole definite dal Codice, nel caso in cui l'amministrazione voglia mantenere al proprio interno questa funzione.

IL CAMBIAMENTO NEL MODO DI OPERARE DELLA PUBBLICA AMMINISTRAZIONE

Le amministrazioni pubbliche sono i principali destinatari del Codice: a loro il compito di intraprendere e rafforzare un percorso virtuoso di innovazione, in molti casi già avviato, per loro l'opportunità di quantificare e di riutilizzare i risparmi ottenuti attraverso l'innovazione tecnologica e organizzativa per incentivare il personale interessato, secondo le norme del d.lgs. 150/09, e per finanziare nuova innovazione.

In questo cambiamento le amministrazioni non sono lasciate da sole: il Codice prevede un accompagnamento costante, attraverso la definizione puntuale di regole tecniche e linee guida di riferimento, attraverso la costituzione di tavoli tecnici specifici e attraverso un affiancamento da parte delle strutture del Ministro per la pubblica amministrazione e l'innovazione, con particolare riguardo all'azione di supporto di DigitPA, cui il Codice riconosce un ruolo fondamentale per l'attuazione del cambiamento.

Questo capitolo intende raccontare alle amministrazioni i nuovi scenari dell'amministrazione digitale individuati dal Codice, evidenziando in particolare quali siano i passi che esse devono percorrere, nei diversi settori, per dispiegare efficacemente l'innovazione.

E' importante ricordare in premessa, come elemento di carattere generale, che il d.lgs. 235/10 lega, per la prima volta, l'innovazione dei processi amministrativi alla valutazione del personale delle amministrazioni, agli incentivi ed alle sanzioni.

Innanzitutto, il Codice dispone che l'osservanza e l'attuazione delle disposizioni previste sia rilevante ai fini della misurazione e della valutazione della performance organizzativa ed individuale dei dirigenti. Per ciascuno degli adempimenti del d.lgs. 235/10 è possibile, pertanto, definire uno o più obiettivi da assegnare ai dirigenti e, dopo aver individuato gli indicatori di misurazione del grado di raggiungimento dell'obiettivo, valutarne la performance come principale condizione per l'erogazione degli incentivi previsti dalla contrattazione integrativa, ai sensi dell'art. 5 del d.lgs. 27 ottobre 2009, n. 150.

Inoltre, le amministrazioni devono quantificare, almeno annualmente i risparmi derivanti dall'innovazione dei processi amministrativi: risparmi che possono essere re-investiti in nuova innovazione o in incentivi con cui motivare il personale coinvolto nell'attuazione del cambiamento. Quindi l'innovazione porta un *dividendo di efficienza* che può essere redistribuito nell'amministrazione.

I paragrafi successivi sono organizzati secondo le principali direttrici del cambiamento individuate dal Codice:

- La gestione dei documenti informatici e dei flussi documentali
- Gli strumenti per verificare l'identità dei cittadini
- SPC: la pubblica amministrazione in rete
- Riutilizzo modulare del software
- Sicurezza dei dati e dei sistemi
- La continuità operativa
- Disponibilità dei dati pubblici

- Realizzazione e diffusione dei servizi in rete

Per ciascun tema sono presentate le principali novità introdotte dal DPCM 235 del 31 dicembre 2010 e gli adempimenti individuati per le amministrazioni.

Nel paragrafo successivo sono presentate le azioni di assistenza ed accompagnamento messe in campo da DigitPA per la tempestiva realizzazione dell'amministrazioni digitale, intervenendo sia a livello di azione tecnica, con la predisposizione dei documenti di approfondimento – regole tecniche e linee guida, sia mediante l'organizzazione momenti di confronto formativo ed informativo rivolti alle amministrazioni.

All'Appendice A è dedicata la descrizione dettagliata dei documenti di approfondimento tecnico che dovranno essere redatti, secondo quanto previsto dall'art. 71 del CAD, sulla base di determinate scadenze, per una definizione puntuale dello scenario tecnologico e normativo di riferimento.

La gestione dei documenti informatici e dei flussi documentali

Le modifiche al Codice dell'Amministrazione Digitale introducono importanti cambiamenti alle norme che disciplinano il valore giuridico dei documenti informatici e le modalità di gestione dei medesimi da parte delle amministrazioni pubbliche; le modifiche introducono inoltre significative novità in merito alle garanzie richieste ai prestatori dei servizi di conservazione.

Riguardo al valore giuridico del documento informatico, la riformulazione dell'articolo 20 del Codice chiarisce che:

- il valore probatorio del documento informatico è liberamente valutabile in giudizio, analogamente all'idoneità dello stesso a soddisfare il requisito della forma scritta;
- l'eventuale data e ora di formazione sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale³;
- la conservazione del documento informatico, in conformità alle regole tecniche, assolve appieno gli eventuali obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente.

Le modifiche apportate al Codice chiariscono il valore giuridico dei documenti informatici ottenuti mediante copia di file, trasmissione via e-mail, funzione di download/upload, ecc. Il codice definisce i documenti ottenuti con queste modalità come “duplicati” (il duplicato è definito appunto nell'art. 1 come “il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario”). L'articolo 23-bis stabilisce che “*i duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti*” purché prodotti in conformità alle regole tecniche. Pertanto, se il documento originario è liberamente valutabile in giudizio, anche il duplicato che si ottiene, ad esempio, mediante l'invio per posta elettronica, sarà liberamente valutabile in giudizio; se invece il documento originario ha l'efficacia della scrittura privata in quanto sottoscritto digitalmente, anche il suo duplicato avrà pari efficacia.

Quando invece si riproduce un documento cambiandone la tipologia o il formato, il Codice ricorre al termine “copia”. A seconda dei casi avremo la copia informatica di documento informatico (ad es. quando si ottiene un nuovo documento cambiando il formato, come nel passaggio da un documento “doc” ad un documento “pdf”), la copia per immagine su supporto informatico di documento analogico (ad es. quando mediante scanner si ottiene un nuovo documento informatico formato dalle immagini di un documento su carta), la copia informatica di documento analogico (ad es. quando attraverso uno scanner con funzione OCR si ottiene un nuovo documento informatico formato dal testo di un documento su carta) e la copia analogica di documento informatico (ad es. quando si genera un documento su carta con la funzione di stampa a partire da un documento informatico).

In tutti questi casi il Codice prevede due regimi:

³ Il DPCM 30 marzo 2009 stabilisce che costituiscono riferimenti temporali opponibili a terzi: la marca temporale generata dai Certificatori accreditati, la data e ora di protocollazione con protocollo elettronico, la data ed ora di conservazione dei documenti ad opera di un pubblico ufficiale o di una pubblica amministrazione, il riferimento temporale ottenuto attraverso l'utilizzo della Posta Elettronica Certifica e le marche postali elettroniche.

- l'attestazione di conformità da parte di un notaio o altro pubblico ufficiale a ciò autorizzato, nel qual caso le copie hanno in ogni caso la stessa efficacia probatoria degli originali;
- l'impiego della copia senza alcuna attestazione, nel qual caso le copie hanno la stessa efficacia probatoria dell'originale se la conformità non è espressamente disconosciuta.

Il regime delle copie in ambito informatico viene dunque allineato a quello delle riproduzioni fotografiche o cinematografiche che formano piena prova dei fatti e delle cose rappresentate se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

L'articolo 22 precisa che le copie per immagine *“sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge”*, il che consente di dematerializzare gli archivi cartacei liberandosi delle enormi quantità di carta che affollano i magazzini. Tuttavia tale regola ha le sue eccezioni: con apposito decreto del Presidente del Consiglio dei Ministri saranno infatti individuate le tipologie di documenti *“per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato”*. Occorre inoltre tenere presente che, fintantoché tali tipologie di documenti non saranno individuate, permane l'obbligo di conservazione degli originali su carta oppure è necessario che un notaio o un pubblico ufficiale attesti la conformità delle copie per immagine a tali originali.

Ai documenti amministrativi, prodotti quindi dalle pubbliche amministrazioni, è dedicato l'articolo 23-ter. dove, tra l'altro, si stabilisce che *“le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico”*. La dematerializzazione dei documenti cartacei nelle pubbliche amministrazioni richiede dunque in ogni caso l'attestazione della conformità delle copie da parte di un funzionario, viene inoltre ribadita la possibilità di liberarsi della carta *“superflua”* restando salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n.42.

Particolarmente importante e innovativa è la disposizione dell'articolo 23-ter comma 5: *“al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico”*. Ciò vuol dire che la stampa di un documento informatico detenuto da un'amministrazione pubblica dovrà

contenere un contrassegno che ne garantisce la conformità all'originale, quindi non sarà più necessario che un cittadino si rechi presso l'amministrazione per ottenere il documento (ad esempio un certificato) ma basterà la stampa ottenibile sulla stampante di casa o presso i sistemi di professionisti e imprese.

Una ulteriore novità che riguarda le pubbliche amministrazioni consiste nell'obbligo di protocollare elettronicamente i documenti scambiati mediante posta elettronica semplice o certificata (limitatamente alle caselle istituzionali), nonché le istanze e le dichiarazioni presentate per via telematica. All'atto pratico tale obbligo si traduce nella necessità di "convogliare" i flussi di documenti veicolati dai sistemi di posta elettronica – in particolare dalla posta Elettronica Certificata – o pervenuti attraverso altri strumenti informatici, nei sistemi di gestione documentale delle pubbliche amministrazioni previsti dal DPR 445/2000 attraverso l'applicazione nota come protocollo informatico. Per adempiere a questa disposizione è opportuno utilizzare applicazioni di protocollo informatico che siano integrabili con i sistemi di posta elettronica e con gli applicativi preposti all'interazione per via telematica con cittadini ed imprese.

Le novità presenti nel nuovo Codice comprendono infine diverse iniziative relative alla conservazione dei documenti informatici. Viene introdotta la figura del Responsabile della conservazione che, operando in raccordo con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ha la responsabilità del mantenimento nel tempo dei documenti informatici. Il responsabile della conservazione può a sua volta avvalersi di *"altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche"* e può richiedere la certificazione della conformità del processo di conservazione ai criteri stabiliti dal Codice e dalle regole tecniche. I soggetti che offrono il servizio di conservazione e forniscono le garanzie di conformità di tale processo ai requisiti del Codice e delle regole tecniche, possono richiedere l'accreditamento a DigitPA che, prima di concederlo, valuterà la sussistenza di requisiti finanziari, organizzativi e tecnici secondo modalità simili a quelle già adottate per l'accreditamento dei Certificatori di firma digitale. DigitPA garantirà poi il corretto svolgimento delle attività di conservazione da parte dei soggetti accreditati attraverso un'attività di vigilanza analoga a quella che già svolge nei confronti dei Certificatori di firma digitale e dei fornitori di Posta Elettronica Certificata. L'istituzione di un elenco di soggetti accreditati a svolgere l'attività di conservazione consentirà, a chiunque ritenga opportuno avvalersi di tali servizi, di scegliere prestatori che hanno dimostrato di possedere i requisiti di qualità e di sicurezza di livello più elevato e che sono soggetti a verifiche periodiche.

Gli adempimenti delle Amministrazioni

L'articolo 40 comma 1 stabilisce che *"le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71"*. Non è sufficiente quindi generare il documento con strumenti informatici, ma occorre che il documento così generato venga trattato come originale. Occorre pertanto abbandonare la prassi – ancora troppo diffusa – dell'uso del personal computer come mera "macchina da scrivere" e della successiva gestione tradizionale del documento stampato; è indispensabile invece che il documento resti informatico e venga gestito in modalità informatica, eventualmente avvalendosi di opportuni prodotti di gestione documentale.

L'impiego di opportuni sistemi di gestione documentale è consigliabile anche per adempiere alla previsione dell'articolo 41, circa la necessità di dotarsi di appositi strumenti per la verifica a distanza da parte del cittadino dell'avanzamento delle pratiche che lo riguardano. Nell'articolo viene infatti ribadito l'obbligo di dotarsi di strumenti che consentano la gestione efficiente dei procedimenti amministrativi utilizzando le tecnologie dell'informazione e la "raccolta" degli atti, documenti e dati del procedimento medesimo in opportuni fascicoli informatici. I sistemi documentali dovranno inoltre integrarsi con i sistemi di protocollo informatico (come già previsto dal DPR 445/2000) che, a loro volta, dovranno essere collegati con tutti i veicoli telematici di scambio di documenti quali: posta elettronica relativa a caselle istituzionali, Posta Elettronica Certificata, strumenti di cooperazione applicativa utilizzati per lo scambio di documenti e applicazioni on line per la presentazione di istanze e dichiarazioni da parte dei cittadini. Il collegamento dovrà essere attuato in modo da consentire l'agevole protocollazione e la successiva gestione dei documenti trasmessi mediante strumenti informatici, evitando così le inefficienze dovute ad una gestione ibrida o totalmente cartacea.

L'amministrazione dovrà organizzarsi affinché i documenti destinati a soggetti esterni all'amministrazione vengano trasmessi o consegnati in modalità elettronica. Questa modalità è obbligatoria nel caso che il destinatario sia un'altra amministrazione, un'impresa, un professionista o un cittadino che ha dichiarato di voler ricevere i documenti in tale forma (ad esempio acquisendo la casella di posta elettronica certificata resa disponibile gratuitamente dal Governo).

Nel caso che il destinatario richieda il documento in forma cartacea, la stampa dovrà essere corredata dal contrassegno elettronico che ne attesta la conformità all'originale detenuto dall'amministrazione.

E' inoltre opportuno che l'amministrazione renda disponibili applicazioni telematiche con cui i cittadini possano insieme inoltrare le richieste alle amministrazioni ed ottenere le eventuali attestazioni o certificazioni in forma elettronica con il contrassegno che ne garantisce l'autenticità, in modo da poter esibire, all'occorrenza, anche la stampa prodotta sulla propria postazione di casa.

Circa la sottoscrizione del documento, le norme attuali consentono di adottare la tecnica più opportuna in funzione dei requisiti di sicurezza e della valenza del documento nell'ambito dell'amministrazione o nei confronti di terzi.

Gli strumenti per verificare l'identità dei cittadini

L'identificazione informatica di un soggetto consiste nella validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad esso, consentendone l'individuazione nei sistemi informativi. L'identificazione deve essere effettuata attraverso opportune tecnologie per garantire la sicurezza dell'accesso.

Secondo l'articolo 64 le amministrazioni possono consentire l'accesso ai servizi online da parte di cittadini e imprese, che richiedono identificazione informatica, oltre che mediante la carta di identità elettronica (CIE) e la carta nazionale dei servizi (CNS), anche utilizzando strumenti diversi di identificazione certa del soggetto richiedente.

In questo contesto diventa particolarmente rilevante la modifica apportata all'art. 65 che prescrive, al comma 1, che istanze e dichiarazioni inviate alle pubbliche amministrazioni per via telematica sono valide e equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento :

- a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;*
- b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;*
- c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente nonché quando le istanze e le dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;*
- c-bis) ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.*

Se precedentemente restava salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione con firma digitale, ora, ai sensi dell'art 65 comma 1-bis, tale facoltà è assunta dal Ministro per la pubblica amministrazione e l'innovazione e dal Ministro per la semplificazione normativa. Pertanto, le pubbliche amministrazioni devono ritenere valide istanze e dichiarazioni presentate con le previste modalità.

Invece, lo scambio di documenti tra amministrazioni è valido ai fini del procedimento amministrativo quando avviene secondo i principi della cooperazione applicativa o quando è possibile verificare la provenienza dei messaggi e documenti scambiati, in base al verificarsi di una delle seguenti condizioni:

- le informazioni sono sottoscritte con firma digitale o con una firma elettronica qualificata;
- le informazioni riportano la segnatura di protocollo conforme alla normativa;

- le informazioni sono trasmesse attraverso la posta elettronica certificata;
- è possibile accertare diversamente la provenienza, sulla base di quanto previsto dalla normativa vigente o dalle regole tecniche;

Appare evidenti il rilievo che dà il Codice alla posta elettronica certificata, con l'obiettivo di rendere questo strumento il principale mezzo di comunicazione per il cittadino nella presentazione di istanze verso le pubbliche amministrazioni, e anche lo strumento che le pubbliche amministrazioni sono tenute ad utilizzare quando a fare richiesta in tale senso è il cittadino stesso. Tale strumento diventa l'unico possibile per le comunicazioni effettuate da e verso le pubbliche amministrazioni da parte delle imprese (art.5 bis).

Le amministrazioni possono accedere e consultare gli elenchi di indirizzi di posta elettronica certificata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali (art. 6)

Vista l'importanza assegnata allo strumento PEC, il Codice prevede sanzioni severe per i Certificatori e per i Gestori di Posta elettronica certificata, finalizzate ad assicurare la continuità di erogazione dei loro servizi e l'impegno a garantire il ripristino in tempi ristretti, in caso di malfunzionamento, salvi naturalmente i casi fortuiti o di forza maggiore che andranno dimostrati (artt. 31 e 32-bis).

Per quanto riguarda la firma elettronica, il Codice definisce quattro tipologie di firme:

1. Firma Elettronica
2. Firma Elettronica Avanzata
3. Firma Elettronica Qualificata
4. Firma Digitale

La **firma elettronica** consente di ricondurre in qualsiasi forma dei dati elettronici ad un soggetto. Il suo valore probatorio è liberamente valutabile in giudizio.

La **firma elettronica avanzata** consente l'identificazione e la connessione univoca al firmatario del documento ed è creata con mezzi sui quali il firmatario può conservare un controllo esclusivo. Consente infine di garantire l'integrità del documento sottoscritto: qualunque modifica invalida la firma. Tale tipologia di firma fa riferimento alla normativa europea in tema di firme elettroniche, secondo quanto indicato dalla Direttiva Europea 1999/93/CE. Il disconoscimento richiede querela di falso.

La **firma elettronica qualificata** è una firma elettronica avanzata certificata da terze parti fidate basata su un certificato qualificato (ovvero conforme ai requisiti della Direttiva Europea 1999/93/CE e rilasciato da un certificatore terzo, che risponde ai requisiti della Direttiva) e realizzata attraverso un mezzo sul quale il firmatario può conservare il controllo esclusivo, quale ad esempio un dispositivo sicuro per la creazione della firma SSCD (Secure Signature Creation Device), quale token, smartcard.... Il disconoscimento richiede querela di falso e soddisfa il requisito della forma scritta ex art.1350 punti da 1 a 12.

La **firma digitale** è una firma elettronica avanzata, basata su un certificato qualificato e su un sistema crittografico asimmetrico (a chiave pubblica). Il disconoscimento richiede querela di falso e soddisfa il requisito della forma scritta ex art.1350 punti da 1 a 12.

La firma digitale “ante modifiche al CAD” essendo basata su un sistema crittografico a chiave pubblica, univa, al SSCD una chiave pubblica a sua volta associata al firmatario da un certificato qualificato. Essa, pertanto, risponde completamente alla definizione di firma elettronica qualificata introdotta dalle modifiche. Viceversa la nuova firma digitale non richiede l’uso del mezzo sul quale il firmatario può conservare il controllo esclusivo, ad esempio in forma di SSCD. Nella Appendice 2 è riportato un quadro sinottico di confronto fra vecchio e nuovo ordinamento il tema di firme elettroniche



Il valore probatorio delle firme elettroniche può essere ricondotto agli articoli 2702, 1350 (punti da 1 a 12) e, per casi particolari, 2703 del codice civile⁴.

4 1350. Atti che devono farsi per iscritto.

Devono farsi per atto pubblico [c.c. 2699] o per scrittura privata [c.c. 2702], sotto pena di nullità [c.c. 812, 1351, 1392, 1403, 1418, 2725]:

- 1) i contratti che trasferiscono la proprietà di beni immobili [c.c. 1470, 1537, 2643, n. 1];
- 2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto [c.c. 978] su beni immobili, il diritto di superficie [c.c. 952], il diritto del concedente [c.c. 960] e dell'enfiteuta [c.c. 957, 959, 2643, n. 2];
- 3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti [c.c. 1100, 2643, n. 2 e n. 3];
- 4) i contratti che costituiscono o modificano le servitù prediali [c.c. 1027, 1051, 1058, 1068], il diritto di uso [c.c. 1021] su beni immobili e il diritto di abitazione [c.c. 1022, 2643, n. 4];
- 5) gli atti di rinuncia ai diritti indicati dai numeri precedenti [c.c. 1070, 2643, n. 5];
- 6) i contratti di affrancazione del fondo enfiteutico [c.c. 971, 2643, n. 7];
- 7) i contratti di anticresi [c.c. 1960, 2643, n. 12];
- 8) i contratti di locazione di beni immobili per una durata superiore a nove anni [c.c. 1108, 1571, 1572, 1573, 1607, 2643, n. 8];

Nella tabella che segue è inquadrato il valore probatorio delle varie tipologie di firme elettroniche.

	Articoli del codice civile applicabili	
	Senza autentica di un pubblico ufficiale	Con autentica di un pubblico Ufficiale
Firma Elettronica	Mero valore probante	2703
Firma Elettronica Avanzata	2702	2702 - 2703
Firma Elettronica Qualificata	1350 commi 1-12- 2702	1350 commi 1-12– 2702 - 2703
Firma Digitale	1350 commi 1-12- 2702	1350 commi 1-12 - 2702 - 2703

Le norme in vigore prevedono che all'interno del certificato qualificato possano essere riportati qualifiche e/o titoli posseduti dal titolare del dispositivo di firma. Detti titoli assumono diverso effetto in dipendenza della presenza dell'indicazione dell'organizzazione di appartenenza.

Se l'organizzazione di appartenenza non è presente, il titolo o qualifica è stato oggetto di dichiarazione sostitutiva di certificazione effettuata dal soggetto ai sensi dell'art. 46 del DPR 445/2000.

L'indicazione dell'organizzazione di appartenenza implica che l'organizzazione ha richiesto al certificatore di rilasciare a tal soggetto un certificato qualificato contenente, oltre all'indicazione dell'organizzazione, il titolo o la qualifica del soggetto. Tale circostanza implica l'obbligo da parte dell'organizzazione di chiedere la revoca del certificato al modificarsi della qualifica.

9) i contratti di società [c.c. 2247, 2251] o di associazione [c.c. 2549] con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato [c.c. 2643, n. 10];

10) gli atti che costituiscono rendite perpetue [c.c. 1862] o vitalizie [c.c. 1872], salve le disposizioni relative alle rendite dello Stato [c.c. 1871, 2643, nn. 1 e 11];

11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari [c.c. 713, 1111, 1113, 1116, 2646];

12) le transazioni [c.c. 1965] che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti [c.c. 2643, n. 13];

2702. Efficacia della scrittura privata.

La scrittura privata [c.c. 1967, 2652, n. 2, 2701, 2705, 2715, 2716, 2821, 2835] fa piena prova [c.c. 1835], fino a querela di falso [c.p.c. 221], della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta [c.c. 2682, n. 3, 2703; c.p.c. 214, 215].

2703. Sottoscrizione autenticata.

Si ha per riconosciuta [c.p.c. 215] la sottoscrizione autenticata [c.c. 2022, 2023, 2206, 2296, 2300, 2333, 2648, 2652, 2702, 2821, 2834, 2835] dal notaio o da altro pubblico ufficiale a ciò autorizzato [c.p.c. 214].

Questa soluzione, pur consentendo di dare un valore aggiunto alla firma del soggetto, implica che si dovranno avere tanti dispositivi quante sono le qualifiche possedute⁵.

Il nuovo CAD prevede che possano essere emessi dei certificati specifici per dichiarare la qualifica di un soggetto⁶. Il soggetto potrà quindi essere dotato di un solo dispositivo di firma cui saranno associati ulteriori certificati secondo necessità. Al decadere di una qualifica, sarà revocato solo il certificato inerente tale qualifica, mentre il soggetto continuerà ad utilizzare lo stesso dispositivo di firma. Questo eviterà la necessità di essere dotati di tanti dispositivi quante sono le qualifiche possedute.

Gli adempimenti delle Amministrazioni

Le amministrazioni sono chiamate ad ottemperare, nel termine di tre mesi dall'entrata in vigore del CAD alla previsione circa l'obbligatorietà dell'utilizzo della PEC (o altre soluzioni analoghe, sempre basate sulle tecnologie dell'informazione e della comunicazione, comunque in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi), in sostituzione delle comunicazioni che richiedono una ricevuta di consegna ai soggetti (ma solo a coloro che hanno preventivamente dichiarato il proprio indirizzo elettronico).

La PEC deve essere integrata nei sistemi di protocollo informatico delle pubbliche amministrazioni, rendendo possibile, a regime, la gestione delle pratiche in modalità totalmente digitale, incluso il controllo dello stato della pratica, grazie alla tracciabilità della stessa (artt. 40-bis e 41).

L'art 47 comma 3 stabilisce anche che, nell'Indice degli indirizzi delle pubbliche amministrazioni – IPA, le amministrazioni devono pubblicare almeno una casella di posta elettronica certificata per ogni registro di protocollo, restando comunque sempre valida l'indicazione dell'art 57-bis secondo cui, i dati relativi agli indirizzi di posta elettronica e o di posta elettronica certificata presenti nell'Indice devono essere aggiornati semestralmente. In IPA devono inoltre essere indicati la struttura organizzativa dell'amministrazione e l'elenco dei servizi offerti nonché le informazioni relative al loro utilizzo.

SPC: la pubblica amministrazione in rete

Le novità principali che riguardano il Sistema pubblico di connettività sono introdotte dagli artt. 75 e 78.

Il comma 3 bis introdotto all'art. 75 del CAD prevede che *“il gestore di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse possono usufruire della connessione al SPC e dei relativi servizi, adeguandosi alle vigenti regole tecniche, previa delibera della Commissione di cui all'articolo 79”*. Tale previsione consente di utilizzare le tecnologie dell'informazione per integrare i procedimenti amministrativi con soggetti privati che

⁵ Sempre riferendosi all'esempio dei notai, questi avranno un certificato in qualità di cittadini, uno in qualità di notai, altri eventuali certificati per altri ruoli rivestiti anche pro tempore.

⁶ Tali certificati sono denominati “certificati d'attributo”.

decidano di adottare le regole tecniche SPC, previa approvazione da parte della Commissione di coordinamento SPC.

Un soggetto privato può utilizzare una connessione ad SPC e, quindi, accedere all'ambito di comunicazione riservato alle amministrazioni, permettendo così alle amministrazioni di comunicare con esso, in una rete protetta senza acquisire connessioni dedicate e senza passare attraverso la rete internet. In questo modo è possibile che un'applicazione informatica appartenente ad un sistema informativo di una PA interagisca con una equivalente appartenente ad un sistema informativo di un privato, estendendo quanto SPC già consente nell'ambito pubblico, cioè di realizzare applicazioni di back office in un ambiente omogeneo, secondo standard definiti, e nell'ambito di prefissate caratteristiche e condizioni di sicurezza.

Il soggetto privato potrebbe inoltre non realizzare un generico scambio informativo con una PA ma usufruire dei servizi infrastrutturali di interoperabilità, cooperazione e accesso, utilizzando le stesse modalità di cooperazione applicativa definite per le amministrazioni, con il reciproco vantaggio di utilizzare tecnologie standard e consolidate (web services) in un ambito sicuro, protetto e con transazioni a valore legale ai sensi dell'art. 76 ovvero: *“gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido ad ogni effetto di legge”*.

L'art. 78, comma 1 del CAD *“Le stesse pubbliche amministrazioni, ove venga loro attribuito, per norma, il compito di gestire soluzioni infrastrutturali per l'erogazione di servizi comuni a più amministrazioni, adottano le medesime regole per garantire la compatibilità con la cooperazione applicativa potendosi avvalere di modalità atte a mantenere distinti gli ambiti di competenza”*, introduce il concetto di un dominio applicativo afferente ad un ambito tematico, dotato di specifiche e distinte infrastrutture e normativamente definito. La previsione, per un dominio siffatto, conclude specificando la possibilità, nell'ambito del rispetto delle regole per la cooperazione applicativa, di poter definire una propria porta di dominio. Le regole tecniche SPC emanate con il DPCM 1 aprile 2008 stabiliscono infatti che ogni dominio applicativo di ciascuna amministrazione definisca una propria porta di dominio, che rappresenta il limite di responsabilità di un'amministrazione ed il componente per il tramite del quale un servizio applicativo di un'amministrazione utilizza il corrispondente di un'altra amministrazione nell'ambito di un predefinito accordo di servizio. La nuova previsione consente di superare quanto definito nelle regole tecniche considerando tali domini come entità equivalenti da un punto di vista delle modalità di cooperazione applicativa alle singole amministrazioni. Si tratta ovviamente di casi molto specifici per i quali la complessità e la criticità è tale da suggerire la predisposizione di infrastrutture specificamente dedicate.

Gli adempimenti delle Amministrazioni

Le amministrazioni, come disposto dallo stesso CAD, oltre che da altri provvedimenti tra i quali la legge n. 2/2009, art. 16, comma 8, sono tenute a dotarsi di caselle di posta elettronica certificata e a predisporre gli interventi di natura tecnico-organizzativa volti a

permettere l'utilizzo delle stesse caselle nell'ambito di procedimenti amministrativi, associandole alle opportune strutture organizzative, uffici di protocollo innanzitutto.

L'articolo 57-bis stabilisce gli obblighi e le associate responsabilità nell'aggiornamento delle informazioni relative all'IPA. La finalità di "trasparenza delle attività istituzionali" che il legislatore ha indicato come primo periodo del comma 1, mira a far conoscere le strutture organizzative responsabili ciascuna per i propri procedimenti ed indirizzare alla struttura specifica la corrispondenza telematica a tutti gli effetti di legge, mediate l'uso delle caselle di posta elettronica certificata, per le comunicazioni tra privati e pubbliche amministrazioni e tra le stesse pubbliche amministrazioni. Ai sensi del comma 3 dell'art. 57 le amministrazioni, in particolare, aggiornano gli indirizzi e le altre informazioni contenute nell'IPA con cadenza almeno semestrale, ed in ogni caso ogni volta che cambia un'informazione rilevante (ad esempio la disattivazione di una casella di posta certificata, una riorganizzazione delle strutture organizzative, il cambio del responsabile dell'amministrazione). Lo stesso articolo prevede che *"la mancata comunicazione degli elementi necessari al completamento dell'indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili"*.

Il Riutilizzo modulare del software

Con il termine di riutilizzo modulare del software ci si riferisce ad un'attività che ha come obiettivo il trasferimento di una soluzione di e-government, intesa come un insieme di servizi – moduli - sviluppati da un'amministrazione e rivolti a cittadini, imprese o altre amministrazioni, o di parti di essa, dall'amministrazione che l'ha progettata e implementata (amministrazione cedente) ad un'amministrazione che desidera implementarla anche nel proprio ambito (amministrazione ricevente o riusante). La tendenza a "riusare" soluzioni modulari già sviluppate da altri enti è un percorso che un numero sempre maggiore di amministrazioni stanno spontaneamente intraprendendo, percependo i vantaggi connessi a tale nuova modalità di sviluppo di innovazione, sia organizzativa sia tecnologica. Vantaggi non solo dal punto di vista di un probabile risparmio di spesa (rispetto ai costi di sviluppo *ex-novo*), bensì anche rispetto alla possibilità di utilizzare e mettere a fattor comune la conoscenza e l'esperienza maturata dall'ente che quella soluzione ha già sviluppato.

Il quadro normativo attinente la pratica del riutilizzo si colloca all'interno del Capo VI - *Sviluppo, acquisizione e riutilizzo di sistemi informatici nelle pubbliche amministrazioni* – con gli articoli dal n.67 al 70. In primis, il Codice estende la pratica del riutilizzo non solo ad interi sistemi e a soluzioni di e-government, ma anche a parti di programmi informatici sviluppati per conto e a spese della amministrazione. Infatti viene introdotto l'obbligo di adottare soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70 del CAD, meglio identificati come *"applicazioni tecnologiche realizzate dalle pubbliche amministrazioni, idonee al riutilizzo da parte di altre pubbliche amministrazioni anche con riferimento a singoli moduli"*. Tali soluzioni, sviluppate per conto e a spese dell'amministrazione, devono quanto possibile essere descritte, documentate e realizzate secondo un concetto di conformità dei programmi già a

partire dai capitolati o dalle specifiche di progetto, alla definizione e regolamentazione effettuata da DigitPA.

Le amministrazioni pubbliche sono tenute a comunicare a DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche e organizzative adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche. Infatti, è proprio sulla base delle di tali comunicazioni che, a seguito di un'attività di confronto e valutazione, DigitPA, realizza e mette a disposizione delle amministrazioni, il catalogo del riuso.

Gli adempimenti delle amministrazioni

Con riferimento alla modifica del comma 1, lettera b) dell'articolo 68, le pubbliche amministrazioni, nel rispetto della legge 7 agosto 1990, n. 241, e del decreto legislativo 12 febbraio 1993, n. 39, che intendono acquisire, secondo le procedure previste dall'ordinamento, programmi informatici a seguito di una valutazione comparativa di tipo tecnico ed economico, devono estendere la medesima, non solo al riuso di programmi informatici, ma anche a parti di essi.

Ai sensi del comma 2 dell'articolo 68, le pubbliche amministrazioni, nella predisposizione o nell'acquisizione dei programmi informatici hanno l'obbligo di adottare soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70 del CAD, meglio identificati come “applicazioni tecnologiche realizzate dalle pubbliche amministrazioni, idonee al riuso da parte di altre pubbliche amministrazioni anche con riferimento a singoli moduli”. E' così che può realizzare un catalogo di *componenti standard* dei programmi informatici della PA, che possono essere riutilizzati e composti l'uno con l'altro secondo le esigenze applicative di ciascuna amministrazione.

L'introduzione del comma 2-bis nell'articolo 68, obbliga le amministrazioni pubbliche a comunicare a DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche e organizzative adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche.

La comunicazione relativa all'adozione delle applicazioni informatiche e delle pratiche tecnologiche e organizzative adottate deve essere tempestiva, per permettere una rapida diffusione di ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti.

Inoltre tale comunicazione deve essere quanto più possibile esaustiva, potendo contemplare, oltre alla descrizione delle applicazioni informatiche o parte di esse, anche le pratiche tecnologiche e organizzative adottate, gli studi di fattibilità, i benchmark, le specifiche tecnico-funzionali, i capitolati tecnici, la documentazione tecnica, i manuali d'uso ed utente, e perfino i risultati ottenuti dalle pubbliche amministrazioni finalizzati a favorire il riuso e la più ampia diffusione delle migliori pratiche

Per effetto del comma 2 dell'articolo 69, le pubbliche amministrazioni che intendono dotarsi di programmi applicativi appositamente sviluppati per conto e a spese delle medesime facilmente portabili su altre piattaforme, devono rendere i capitolati o le specifiche di progetto conformi alla definizione e alla regolamentazione effettuata da DigitPA.

L'obbligo delle conformità è formalmente vincolante per quelle forniture ICT che, ai sensi della normativa vigente e con specifico riferimento a quanto stabilito nell'art.67 del CAD, "Modalità di sviluppo ed acquisizione", devono essere sottoposte a parere di congruità da DigitPA.

Quando le pubbliche amministrazioni, nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, ai sensi del comma 4 dell'articolo 69, intendono includere clausole, concordate con il fornitore, che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso dei programmi o dei singoli moduli, devono espressamente fare riferimento ai programmi informatici o a parti di essi.

La sicurezza dei dati e dei sistemi

L'art.2 del Codice afferma che "lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione".

In questo contesto e con tali finalità, gli aspetti di sicurezza assumono un ruolo trasversale rispetto all'articolato del Codice: le informazioni gestite dai sistemi informativi pubblici, infatti, costituiscono una risorsa di valore strategico per il governo del Paese ed è responsabilità dello Stato e singolarmente di tutte le amministrazioni che lo compongono, centrali e locali, proteggere questo patrimonio quale presupposto per il suo funzionamento, a servizio di cittadini ed imprese.

Ai sensi dell'art. 12, co. 2, *"Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71"*

Se queste previsioni rimangono invariate con la nuova formulazione del CAD, alcune previsioni inerenti gli aspetti di sicurezza rappresentano una novità, e precisamente:

- art. 17: ***Strutture per l'organizzazione, l'innovazione e le tecnologie***, che prevede l'individuazione di un ufficio di livello dirigenziale con competenze di coordinamento anche degli aspetti di sicurezza;
- art. 51: ***Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*** che affida ad un successivo provvedimento normativo di secondo livello la definizione delle modalità necessarie a garantire la

sicurezza IT nella PA e, a tal fine, attribuisce a DigitPA una serie di competenze necessarie alla concreta realizzazione degli obiettivi di sicurezza;

- **norme transitorie e finali** che abrogano il centro di competenza di cui alla normativa previgente e il responsabile dei sistemi informativi automatizzati di cui all'articolo 10 del decreto legislativo 12 febbraio 1993, n. 39,

Adempimenti delle Amministrazioni

L'impianto complessivo del Codice in materia di sicurezza contiene numerosi riferimenti diretti ed indiretti agli aspetti di sicurezza informatica che interessano nel dettaglio singole tematiche (come il documento digitale, la firma elettronica o la posta elettronica certificata) e che comunque individuano ruoli e responsabilità secondo un modello verticistico ed uniforme per tutte le Amministrazioni. Infatti, l'art. 14 dispone che *“Lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.”*

Nell'ambito delle rispettive responsabilità, pertanto, il CAD sancisce che ciascun ente sia chiamato a realizzare politiche idonee garantire integrità, la disponibilità e affidabilità dei dati e delle informazioni trattati, ma individua ed attribuisce compiti regolatori e d'indirizzo al Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie: *“Per il perseguimento dei fini di cui al presente codice, il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie, nell'attività di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle pubbliche amministrazioni centrali per lo sviluppo dei sistemi informativi, detta norme tecniche ai sensi dell'articolo 71 e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle pubbliche amministrazioni centrali e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi e della loro sicurezza (art. 16 lett. e).*

La sicurezza informatica è un fattore abilitante dell'azione amministrativa, tanto importante quanto la digitalizzazione stessa, e per questo il Codice definisce un sistema organico di ruoli e responsabilità che supera il precedente modello introdotto con il D.lgs nr.39 del 1993⁷ e la Direttiva Stanca (DM 16.01.2002)⁸.

Coerentemente con quest'architettura, le singole amministrazioni hanno l'onere di identificare l'organismo interno responsabile delle iniziative intraprese dall'amministrazione in materia di digitalizzazione, anche con specifico riferimento alla sicurezza, ed in particolare per quanto riguarda l'indirizzo, la pianificazione, il coordinamento e il monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture.

⁷ Che imponeva ad ogni amministrazione di identificare un Responsabile dei Sistemi informativi automatizzati (RSIA) da comunicare all'AIPA.

⁸ Con questo provvedimento normativo di secondo livello era stato identificato un modello di organigramma e di distribuzione di funzioni in materia di sicurezza ICT uniforme per tutti i ministeri.

Tutto ciò è coerente con i principi fondamentali di sicurezza e consente per la prima volta di identificare una reale *governance* della sicurezza informatica nella PA, sempre attribuita al Capo all'Esecutivo o al Ministro da questi delegato⁹, cui corrisponde (ecco la novità!) un ufficio di livello dirigenziale interno all'amministrazione¹⁰ e competente per tutti gli aspetti di gestione operativa delle attività di sicurezza informatica. Per la prima volta, dunque, si obbligano le amministrazioni ad identificare, entro 120 gg. dall'entrata in vigore del CAD, un dirigente responsabile della sicurezza informatica, con diretto riferimento ai dati, ai sistemi ed alle infrastrutture, anche in relazione al Sistema pubblico di connettività.

Alle competenze dell'ufficio dirigenziale potranno, quindi, essere ricondotte le funzioni previste in capo all'Unità Locale di Sicurezza SPC, la componente distribuita del Sistema Pubblico di Connettività istituita in ogni amministrazione, che assicura il rispetto delle regole e delle politiche di sicurezza previste dall'art.21 del DPCM 01.04.2008 (Regole Tecniche e di funzionamento di SPC).

La continuità operativa

La crescente complessità delle attività legate alla Pubblica Amministrazione, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio, quali quelli determinati da un attacco di tipo terroristico o anche solamente malevolo, così come gli inconvenienti di natura tecnica, che possono portare all'interruzione totale dei servizi istituzionali anche per lunghi periodi, evidenziano, l'esigenza che le amministrazioni aggiornino il livello di predisposizione a questi potenziali fermi della propria operatività.

In questa direzione, è quindi necessario che le pubbliche amministrazioni adeguino le strategie in tema di sicurezza e rafforzino i presidi di emergenza in modo da garantire la continuità di funzionamento dei sistemi informativi attraverso i quali le stesse PA assicurano lo svolgimento dei rispettivi compiti istituzionali e l'erogazione dei servizi all'utenza.

Le pubbliche amministrazioni devono quindi dotarsi di strumenti, accorgimenti e procedure per assicurare la Continuità Operativa (CO), intesa come *“insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale”*, per far fronte a incidenti di ampia portata o a eventi imprevisti che comportano l'indisponibilità del proprio sistema Informativo al fine di evitare fermi o gravi interruzioni della propria operatività con impatti negativi o disservizi nei procedimenti svolti e nei servizi erogati all'utenza.

In questo scenario generale la continuità operativa dei sistemi informativi rappresenta per le pubbliche amministrazioni il punto nevralgico necessario all'erogazione dei servizi a cittadini e imprese.

E' pertanto indispensabile assicurare la continuità dei servizi per garantire il corretto svolgimento della vita nel Paese, anche in presenza di eventi imprevisti, ai quali si è

⁹ Attraverso l'emanazione di Regole Tecniche previste dall'art.71 del testo in commento.

¹⁰ Non più un generico *centro di competenza*, come previsto nella precedente formulazione.

finora fatto fronte, generalmente, ricorrendo a soluzioni di emergenza di tipo tradizionale quali spostamento di personale tra uffici, attivazione di procedure manuali in sostituzione di quelle informatizzate temporaneamente sospese e altre misure simili.

Le soluzioni per garantire la continuità operativa dei sistemi informativi non considerano soltanto le componenti tecnologiche utilizzate ma anche tutte le altre risorse (personale, impianti, ecc.). La continuità operativa considera i mezzi tecnici impiegati nei procedimenti amministrativi come strumenti per l'erogazione dei servizi ed estende la sua sfera di interesse a tematiche più generali di natura organizzativa.

Componente fondamentale della continuità operativa dei sistemi informativi è poi il disaster recovery, inteso come l' "insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso".

In base a queste e altre considerazioni, è stata colta l'occasione della revisione del CAD per inserire in tale revisione un nuovo articolo, il 50-bis "Continuità operativa", l'unico nella revisione che non riprenda disposizioni già presenti nel vecchio testo e che è specificatamente rivolto a questo importante aspetto infrastrutturale.

In sintesi, l'articolo prevede:

- la predisposizione di un piano di continuità (comma 3, punto a)), inclusivo del piano di disaster recovery (comma 3, punto b)), da parte di tutte le pubbliche amministrazioni;
- la stesura, preventiva al precedente adempimento, di un apposito studio di fattibilità, sul quale deve essere obbligatoriamente richiesto parere a DigitPA (comma 4).

Gli adempimenti delle Amministrazioni

Come previsto all'articolo 57 "Norme transitorie e finali", comma 10: *" Le pubbliche amministrazioni provvedono a definire i piani di cui all'articolo 50-bis del decreto legislativo 7 marzo 2005, n. 82, come introdotto dall'articolo 34, [i piani di continuità operativa e di disaster recovery], entro quindici mesi dalla data di entrata in vigore del presente decreto".*

Le Amministrazioni devono preventivamente predisporre uno studio di fattibilità propedeutico alla produzione del piano di continuità, per il quale devono richiedere obbligatoriamente parere a DigitPA. In sintesi, lo studio di fattibilità deve contenere:

- la descrizione dell'architettura informatica dell'Amministrazione che comprende: la descrizione del contesto tecnico operativo del sistema informativo primario, le componenti hw e sw dell'architettura, le applicazioni, le basi di dati; i procedimenti istituzionali e strumentali che si avvalgono o si svolgono attraverso il Sistema Informativo; la tipologia di utenti (interni, esterni); i servizi on line erogati;

- l'organizzazione dei servizi informatici e le modalità con cui l'Amministrazione si assicura la gestione, manutenzione ed evoluzione del proprio sistema informativo;
- le politiche e le relative misure di sicurezza adottate: le pratiche di salvataggio dei dati adottate per assicurare il salvataggio dei dati, indicandone modalità, termini, cadenza, nonché le modalità di conservazione, custodia ed eventuale utilizzo delle copie di back up;
- l'analisi degli impatti sulla operatività della amministrazione e dei conseguenti scenari di crisi, con particolare riferimento ai servizi critici;
- i requisiti di continuità, ritenuti necessari alla luce dell'analisi di impatto, per i servizi critici e per le risorse informatiche a supporto in termini di RTO¹¹ e di RPO¹²;
- l'identificazione dei "gap" tra requisiti di continuità operativa e la situazione attuale del sistema informativo; questo permetterà di valutare anche l'eventuale presenza di soluzioni già adottate;
- le possibili strategie e soluzioni di continuità con stima di costi e benefici;
- la soluzione tecnico organizzativa proposta; la soluzione adottata per assicurare il ripristino dell'operatività, con quali componenti e configurazioni di emergenza, con quali tempi di RTO e RPO, con quali modalità di replica (sincrona; asincrona; a caldo, a freddo ecc.);
- le modalità di monitoraggio e controllo della soluzione e di verifica della costante adeguatezza della soluzione stessa, comprensiva degli accorgimenti organizzativi e procedurali adottati a tal fine;
- la pianificazione (tempi e risorse previsti) per la piena realizzazione di quanto disposto dal CAD per la continuità operativa.

Il Piano di continuità operativa deve contenere almeno:

- l'analisi del contesto, l'individuazione dei servizi critici, l'esito delle valutazioni del rischio e dell'impatto di indisponibilità dei sistemi informativi, la descrizione dei requisiti di continuità operativa che si devono assicurare;
- la soluzione e le strategie di riduzione del rischio e di ripristino in caso di emergenza
- le misure tecnico organizzative e le procedure definite per la gestione della continuità operativa e per la gestione dell'emergenza (come da piano di disaster recovery).

La funzionalità del piano di continuità operativa deve essere verificata, da parte delle amministrazioni, con cadenza biennale, mentre l'omogeneità delle soluzioni indicate nei diversi piani è assicurata dal Ministro per la pubblica amministrazione e l'innovazione, che ne informa con cadenza almeno annuale il Parlamento.

¹¹ RTO (Recovery Time Objective) massimo tempo di indisponibilità del servizio, ovvero tempo entro il quale il servizio da proteggere deve essere ripristinato

¹² RPO (Recovery Point Objective) perdita dati sostenibile, in termini di distanza temporale tra il verificarsi dell'emergenza e l'ultimo salvataggio utile dei dati

Il Piano di disaster recovery deve contenere almeno:

- la struttura organizzativa per la gestione dell'emergenza e del piano;
- le procedure di ripristino, in caso di emergenza, dell'operatività del sistema informativo nei siti alternativi a quelli di produzione e procedure per il successivo rientro dalla situazione di emergenza
- le modalità di test, aggiornamento e miglioramento del piano.

Le amministrazioni devono inviare a DigitPA i piani di disaster recovery, unitamente a un prospetto sintetico che evidenzia le principali variazioni apportate con le relative motivazioni (ad esempio: adozione di nuove piattaforme tecnologiche, variazione dei requisiti di continuità operativa). DigitPA verifica annualmente il costante aggiornamento dei piani di disaster recovery delle Amministrazioni e ne dà informazione al Ministro per la pubblica amministrazione e l'innovazione.

Disponibilità dei dati pubblici

L'informazione pubblica, ossia l'insieme delle informazioni e dei dati raccolti, prodotti e gestiti dalla pubblica amministrazione nell'esercizio delle proprie attività istituzionali, rappresenta una risorsa che deve essere disponibile sia a tutte le amministrazioni sia ai cittadini. La sua valorizzazione consente non solo lo sviluppo della partecipazione e della trasparenza e l'efficace esercizio dell'attività amministrativa, ma può contribuire anche allo sviluppo sociale ed economico del paese. Essa ha, infatti, una significativa valenza economica, sia come possibilità di commercializzazione a diretto vantaggio dello stato, sia come supporto alla crescita economica e produttiva, una volta messa a disposizione di operatori che possano utilizzarla per confezionare nuovi servizi da veicolare sul mercato. La disponibilità in formato elettronico delle informazioni e dei dati pubblici ne facilita l'accesso, l'interscambio e la fruibilità e ne accentua sostanzialmente le possibilità di effettivo utilizzo e valorizzazione, altrimenti spesso soltanto teorica.

I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione. L'informazione pubblica deve essere valorizzata attraverso progetti di elaborazione e diffusione dei dati, che possono essere finanziati dalle amministrazioni ricorrendo a strumenti di finanza di progetto.

Oltre ad aggiornare tempestivamente i dati dei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi, le amministrazioni devono consentire l'accesso gratuito alle banche dati accessibili per via telematica di cui sono titolari. Tale accesso deve essere disciplinato mediante apposite convenzioni da stipulare con le amministrazioni interessate. Anche i dati pubblicati sui siti pubblici devono essere fruiti gratuitamente e devono inoltre essere resi disponibili secondo un formato aperto.

Fra i dati gestiti dalla pubblica amministrazione, il Codice assegna una particolare rilevanza al tema dei dati territoriali. Per dato territoriale si intende qualunque informazione geograficamente localizzata. La conoscenza del dato territoriale, nei suoi

vari aspetti, è determinante sia come strumento per lo sviluppo di nuovi servizi sia come supporto alle decisioni in molteplici campi. Basti pensare alle politiche di sicurezza, di protezione civile, agricoltura, pianificazione territoriale, trasporti, ambiente, catasto, governo del territorio, gestione delle infrastrutture, sviluppo economico, reti tecnologiche, ecc., con ricadute significative anche sul terreno della fiscalità.

In Italia sono molte le materie “concorrenti” spesso distribuite tra più soggetti: numerosi Enti o Amministrazioni raccolgono, producono o gestiscono dati territoriali in funzione delle proprie competenze istituzionali. L’informazione territoriale è quindi caratterizzata da un consistente patrimonio di dati e, contestualmente, da una significativa frammentazione non strutturata e da molteplici sovrapposizioni.

E’ dunque fondamentale definire regole e standard idonei a far sì che:

- a) l’informazione territoriale, una volta acquisita, possa essere usufruibile da parte di tutte le amministrazioni interessate e che ad essa possano avere accesso imprese e professionisti in relazione alle evidenti implicazioni di sviluppo di attività produttive
- b) il sistema pubblico possa operare in modo collaborativo, ottimizzando le risorse economiche a disposizione e massimizzando i risultati conseguibili.

Proprio con queste finalità l’articolo 59 del CAD ha istituito:

- il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, con il compito di proporre regolamenti e norme tecniche per la standardizzazione dell’informazione territoriale, sia in fase di acquisizione, sia di utilizzo.
- Il Repertorio nazionale dei dati territoriali, concepito come strumento idoneo ad agevolare la pubblicità, la conoscenza e la ricerca delle informazioni territoriali possedute dalle pubbliche amministrazioni.

Il Repertorio nazionale dei dati territoriali fa parte delle “basi di dati di interesse nazionale”, assumendo quindi le caratteristiche che il nuovo articolo 60 del CAD prevede per tali basi di dati, la cui conoscenza è utilizzabile dalle pubbliche amministrazioni, anche per fini statistici, per l’esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti.

Più o meno contemporaneamente, anche in Europa si è avvertita la necessità di favorire l’interoperabilità, nel settore dell’informazione geografica in particolare. Infatti con la direttiva 2007/2/CE (nota come direttiva Inspire), recepita nell’ordinamento nazionale con il D. Lgs. 32/2010, pur traendo origine in un contesto di politica ambientale, viene istituita un’infrastruttura per l’informazione territoriale nella Comunità europea, delineando un quadro di riferimento a livello europeo cui tutti i paesi sono tenuti ad aderire sia in termini tecnici che regolamentari.

In conclusione, attraverso i succitati strumenti il CAD mira alla acquisizione della consapevolezza circa il potenziale anche economico dell’informazione territoriale come volano per lo sviluppo di iniziative e di competitività in molti dei settori sopra citati, operando fattivamente in maniera coordinata con l’intento di realizzare misure e

strumenti condivisi ed efficaci, per valorizzare il patrimonio pubblico dell'informazione geografica.

Gli adempimenti delle amministrazioni

Ai sensi dell'art 58 comma 2, le amministrazioni devono redigere, sulla base delle Linee guida predisposte da DigitPA, le convenzioni per consentire l'accesso alle banche dati di cui sono titolari.

Devono inoltre pubblicare secondo formati aperti, definiti cioè da specifiche pubbliche non proprietarie, liberamente accessibili, senza restrizioni legali per l'utilizzo, e rendere fruibili gratuitamente le informazioni sui propri siti web.

Con riferimento alle attività del Comitato, le amministrazioni che producono acquisiscono o gestiscono dati territoriali devono tenere conto delle regole tecniche predisposte dal Comitato medesimo.

Per quanto riguarda invece il Repertorio nazionale dei dati territoriali, le amministrazioni sono tenute a documentare i propri dati territoriali, e relativi servizi, attraverso il conferimento dei pertinenti metadati nel Repertorio medesimo. Detto Regolamento, in sintonia con i principi e gli obiettivi perseguiti attraverso il CAD, prevede inoltre l'obbligo da parte di un'amministrazione che intende intraprendere un'attività di acquisizione di dati territoriali, di documentare nel Repertorio le caratteristiche del prodotto previsto, attivando così un processo di pianificazione volto a verificare l'eventuale esistenza di esigenze comuni da parte di altre amministrazioni e la possibilità di attivazione di specifici accordi di collaborazione, con conseguente riduzione dei costi complessivi e ottimizzazione delle risorse necessarie.

Realizzazione e diffusione dei servizi in rete

Le amministrazioni devono mettere a disposizione di cittadini ed imprese servizi erogati con modalità telematica: servizi in rete, tipicamente accessibili attraverso il sito web dell'amministrazione. L'art 63 indica alle PA i criteri a cui deve essere improntata la progettazione, la realizzazione e la conduzione dei servizi in rete:

- Considerazione delle esigenze degli utenti del servizio, con particolare attenzione a condizioni di disagio, in base a principi di uguaglianza e non discriminazione;
- valutazione di economicità, efficacia e utilità, anche sulla base della frequenza d'uso del servizio e del bacino di utenza previsto;
- tracciabilità e completezza del procedimento avviato on-line;
-
- rilevazione continua e sicura del grado di soddisfazione degli utenti.

Canale principale per l'accesso, da parte di cittadini ed imprese, ai servizi in rete, è il sito web, istituzionale o tematico, dell'amministrazione, a cui il Codice dedica gli articoli 53, 54 e 57 del Capo V - *Dati delle pubbliche amministrazioni e servizi in rete*.

In particolare, le modifiche introdotte dal Codice riguardano la definizione delle caratteristiche dei siti delle amministrazioni, che devono essere realizzati secondo i principi di accessibilità, usabilità, reperibilità e completezza delle informazioni, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità, tenendo con che i dati pubblici contenuti nei siti delle amministrazioni devono poter essere fruiti dai cittadini in modo gratuito e senza necessità di identificazione informatica. Il Codice prevede inoltre l'ampliamento dei contenuti obbligatori dei siti istituzionali, rendendo obbligatoria la pubblicazione integrale dei bandi di concorso e non più solo l'elenco di essi.

Le amministrazioni devono pubblicare sul sito istituzionale un indirizzo di posta elettronica certificata, a cui i cittadini possano rivolgersi per qualsiasi comunicazione con l'amministrazione, secondo le modalità indicate nello stesso Codice e devono rendere noti i tempi di risposta alle richieste pervenute a tale indirizzo PEC. Inoltre deve essere pubblicato sul sito del registro dei processi automatizzati rivolti al pubblico, che devono essere dotati di appositi strumenti attraverso cui i cittadini possano verificare l'avanzamento delle pratiche che li riguardano. Le amministrazioni devono infatti garantire la conformità e la corrispondenza delle informazioni contenute sui siti rispetto alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito.

Sul sito istituzionale deve essere pubblicato l'elenco dei documenti richiesti per avviare un procedimento (compresi moduli e formulari) che non potranno in alcun modo essere richiesti al cittadino qualora non siano stati pubblicati sul web e la mancata pubblicazione è rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili del procedimento di pubblicazione.

Gli adempimenti delle amministrazioni

Ai sensi dell'art. 54 comma 1, le amministrazioni devono rendere disponibili, sui propri siti istituzionali, le seguenti informazioni¹³:

- l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio anche di livello dirigenziale non generale, i nomi dei dirigenti responsabili dei singoli uffici, nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, corredati dai documenti anche normativi di riferimento;
- l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241;

¹³ Si ricorda che oltre ai contenuti obbligatori previsti dal CAD, le amministrazioni sono tenute a pubblicare sui propri siti istituzionali altre informazioni, secondo quanto previsto dalla L.150/2000, dal DPR 23 aprile 2004 n° 108, dalla Legge n 69/2009, dal D.Lgs 150/2009.

- le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241;
- l'elenco completo delle caselle di posta elettronica istituzionali attive, specificando anche se si tratta di una casella di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;
- le pubblicazioni di cui all'articolo 26 della legge 7 agosto 1990, n. 241, nonché i messaggi di informazione e di comunicazione previsti dalla legge 7 giugno 2000, n. 150;
- l'elenco di tutti i bandi di gara;
- i bandi di concorso;
- l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando tempi previsti per l'attivazione medesima.

Inoltre, secondo l'art 54 comma 2-ter, le amministrazioni devono pubblicare sul sito istituzionale un indirizzo di posta elettronica certificata, a cui i cittadini possano rivolgersi per l'invio di qualsiasi istanza telematica, secondo le modalità previste dalla normativa.

Le amministrazioni devono assicurare che i dati ed i documenti pubblicati siano in formato aperto¹⁴, secondo quanto stabilito all'art 52 comma 1-bis e 68 comma 4.

Ai sensi dell'art 54 comma 1-bis, le amministrazioni centrali devono inviare per via telematica al Dipartimento della Funzione Pubblica, che provvederà a pubblicarli sul proprio sito istituzionale, i dati pubblicati relativi a:

- l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241;
- le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241;
- l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando tempi previsti per l'attivazione medesima.
- i bandi di concorso

Le amministrazioni devono definire e rendere disponibile per via telematica, ai sensi dell'art 57 comma 1, la documentazione necessaria per i singoli procedimenti, compresi

¹⁴ Un formato aperto è definito da specifiche pubbliche non proprietarie, liberamente accessibili, senza restrizioni legali per l'utilizzo.

moduli ed formulari, permettendo ai cittadini, in caso di omessa pubblicazione, l'avvio dei procedimenti in assenza di tali moduli e formulari (art 57 comma 2).

I pagamenti Elettronici

La completa revisione dell'art. 5 (*Effettuazione di pagamenti con modalità informatiche*) operata dal nuovo Codice dell'Amministrazione digitale si colloca nell'ambito delle attività intraprese a livello nazionale dalle istituzioni di riferimento del sistema paese che hanno avviato iniziative volte a modernizzare e rendere più efficiente la Pubblica Amministrazione attraverso l'attuazione di iniziative strategiche specificate nel piano e-gov 2012.

L'esigenza ormai non più rinviabile è quella di mettere a disposizione delle pubbliche amministrazioni tutti gli strumenti di pagamento elettronici per consentire a queste ultime di rivedere l'offerta dei propri servizi attraverso procedure informatiche che permettono in via automatica l'operazione di pagamento nelle diverse forme e canali oggi esistenti.

Nella versione precedente l'articolo 5 era composto da un unico comma che tracciava degli indirizzi di carattere generale, mentre ora l'articolo è composto da 4 commi, il primo dei quali allarga a tutte le pubbliche amministrazioni l'obbligo di consentire il pagamento ai privati attraverso canali informatici (prima tale obbligo era limitato alle sole amministrazioni centrali) e ne circoscrive il perimetro, escludendo da tale attività quelle legate alla riscossione dei tributi e regolate da specifiche normative.

Il nuovo comma 2 dell'articolo 5 detta disposizioni in merito alle sole pubbliche amministrazioni centrali, che possono avvalersi di prestatori di servizi di pagamento (Banche, Poste, Istituti di moneta elettronica e Istituti di pagamento, come previsto dalla Direttiva comunitaria sui servizi di pagamento) per consentire ai privati di effettuare i pagamenti in loro favore.

Lo stesso comma 2 pone il vincolo alle amministrazioni di esercitare tali attività senza che da queste ne scaturiscano nuovi o maggiori oneri per la finanza pubblica e traccia le linee di indirizzo circa il processo di riversamento presso l'erario delle somme incassate; tale processo dovrà essere regolamentato attraverso un decreto da emanarsi a cura del Ministro per la pubblica amministrazione e l'innovazione e i Ministri competenti per materia, di concerto con il Ministro dell'economia e delle finanze, sentito DigitPA (nuovo comma 3).

Infine il nuovo comma 4 ribadisce l'obbligo, per gli enti locali e le Regioni (compresi i propri enti e le amministrazioni del Servizio sanitario nazionale), di mettere a disposizione dei privati strumenti e canali informatici per consentire il pagamento delle somme dovute.

Gli adempimenti delle Amministrazioni

Gli adempimenti per le amministrazioni saranno stabiliti all'interno del decreto che dovrà essere emanato a norma del comma 3; in linea di massima tali obblighi potranno riguardare:

- le infrastrutture necessarie per collegarsi al Sistema dei pagamenti per colloquiare con i prestatori di servizi di pagamento;
- gli strumenti per consentire al debitore di effettuare i pagamenti informatici e per conservare digitalmente le informazioni correlate;
- gli strumenti per riprodurre su supporti diversi, a richiesta e cura del debitore, l'attestazione dell'avvenuto pagamento, comprensiva dei dati identificativi dello stesso;
- l'integrazione dei pagamenti con i propri processi amministrativi;
- la messa a disposizione, ove il privato lo richieda, di una casella di posta elettronica per comunicare l'esito dei pagamenti (ai sensi del D.L. 29 novembre 2008, n. 185 convertito in legge, con modificazioni, dall'art. 1, L. 2 del 28 gennaio 2009).

L'accompagnamento di DigitPA

DigitPA, nell'ambito dei propri compiti istituzionali di consulenza e proposta, nonché di valutazione, di monitoraggio e di coordinamento, fornisce un concreto supporto alle Amministrazioni al fine di agevolare il processo di attuazione del Codice.

Il Codice affida a DigitPA il compito di accompagnamento per la tempestiva realizzazione dell'amministrazioni digitale, intervenendo sia a livello di azione tecnica, con la predisposizione dei documenti di approfondimento – regole tecniche e linee guida – previsti dal CAD, sia mediante l'organizzazione momenti di confronto formativo ed informativo rivolti alle amministrazioni. Tale compito si inquadra nel più generale ruolo di DigitPA, individuato dal D.Lgs 177/2009, a supporto del percorso di innovazione della PA, per cui l'Ente mette a disposizione delle amministrazioni le proprie competenze tecniche, stipulando accordi quadro per mettere a disposizione delle amministrazioni i servizi innovativi, formulando pareri sui contratti stipulati dalle PA centrali, monitorando i piani ICT delle Amministrazioni e pubblicando linee guida sulla qualità dei beni e dei servizi ICT.

Le amministrazioni, dunque, si potranno avvalere anche per l'attuazione del CAD dell'assistenza tecnica di DigitPA, che imposterà, sulla base delle esigenze organizzative e tecnologiche di ciascuna amministrazione, specifiche azioni di supporto ed accompagnamento, secondo una *roadmap* di assistenza, avviata sin dal momento dell'entrata in vigore del Codice

Il supporto si articola in:

- redazione di documenti tecnici (ie regole tecniche e linee guida);
- consulenza nell'applicazione delle norme;
- illustrazione degli impatti dell'innovazione sul personale e sulle organizzazioni e consulenza nella scelta delle soluzioni organizzative più appropriate;
- assistenza al cambiamento;
- formazione rivolta al personale delle Amministrazioni;
- accreditamento dei prestatori dei servizi qualificati e vigilanza sui medesimi
- controllo e monitoraggio sui gestori del servizio di posta elettronica certificata
- stipula di accordi quadro in un ottica multi fornitore, in considerazione anche di aspetti di apertura del mercato e concorrenza

Inoltre, DigitPA, rispetto alle tematiche individuate dal Codice:

- cura la progettazione realizzazione e la gestisce delle infrastrutture nazionali condivise del SPC, impegnandosi in attività di realizzazione, di implementazione delle linee guida e di supporto a tutte le amministrazioni nell'adozione delle medesime linee guida e dei servizi infrastrutturali.
- presiede la Commissione di coordinamento SPC
- realizza, gestisce e aggiorna l'Indice degli indirizzi delle pubbliche amministrazioni, IPA. L'IPA è raggiungibile attraverso il sito www.indicepa.gov.it che espone le funzionalità di interfaccia sia verso privati e PA per la consultazione, sia verso le PA per le funzioni di inserimento e modifica

- effettua azioni di monitoraggio e verifica del rispetto delle disposizioni relative all'utilizzo dei servizi di voce tramite protocollo internet (VoIP) da parte delle amministrazioni centrali, scuole ed università
- provvede all'aggiornamento del documento "Guida alla firma digitale
- emette pareri sugli studi di fattibilità propedeutici alla produzione dei piani di continuità e di Disaster Recovery;
- verifica annualmente il costante aggiornamento dei piani di disaster recovery e informa il Ministro per la pubblica amministrazione e l'innovazione dell'esito di queste verifiche;
- realizza e gestisce la banca dati dei programmi informatici riusabili;
- cura la realizzazione e la gestione del portale del Repertorio nazionale dei dati territoriali;
- partecipa alle attività del Comitato per le regole tecniche sui dati territoriali sia come componente di tale organismo, sia per l'espletamento delle funzioni di segreteria tecnica e lo svolgimento dei compiti istruttori, di studio e di supporto tecnico scientifico.

Nell'Appendice A, sono riportati in dettaglio i documenti - regole tecniche e linee guida - previsti dal Codice per ciascuna delle aree di cambiamento descritte in precedenza. Tali documenti tecnici, emanati, in molti casi, attraverso decreti del Presidente del Consiglio dei Ministri, vedranno la collaborazione di tutti gli stakeholders pubblici e privati interessati attraverso l'istituzione di tavoli di lavoro e di consultazione e saranno pienamente integrati con quanto già emanato nell'ambito del Sistema pubblico di connettività e cooperazione.

APPENDICE A – DOCUMENTI DI APPROFONDIMENTO TECNICO: REGOLE TECNICHE E LINEE GUIDA

Regole tecniche per la formazione, tenuta e conservazione del documento informatico.

Saranno emesse entro il 25 gennaio 2012 con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali e la Conferenza unificata, sentiti DigitPA e il Garante per la protezione dei dati personali. Disciplinano la formazione del documento informatico, la sua memorizzazione su supporto informatico, la modalità di trasmissione, le copie e l'eventuale attestazione di conformità, la duplicazione e riproduzione, la generazione di estratti su supporto informatico o analogico, la stampa con contrassegno informatico, il recupero su supporto informatico dei documenti e degli atti cartacei, la conservazione e l'esibizione dei documenti tenuti o conservati.

Regole tecniche per il protocollo informatico e per la gestione dei flussi documentali.

Saranno emesse in attuazione dell'articolo 71 del Codice dell'Amministrazione Digitale con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali e la Conferenza unificata, sentiti DigitPA e il Garante per la protezione dei dati personali. Aggiungeranno le vigenti regole tecniche per il protocollo informatico (DPCM 31 ottobre 2000) per tenere conto delle novità introdotte dal Codice. Riguarderanno l'organizzazione della gestione documentale, i compiti del responsabile del servizio per la tenuta del protocollo informatico e del responsabile della conservazione, la segnatura di protocollo, la gestione dei documenti con strumenti informatici, la formazione del fascicolo informatico, la gestione dei procedimenti amministrativi attraverso l'automazione dei flussi documentali, le modalità di integrazione dei sistemi documentali con i sistemi di posta elettronica e di cooperazione applicativa conformi agli standard SPC, nonché con le applicazioni on line per la ricezione di istanze e dichiarazioni da parte dei cittadini.

Linee guida per la generazione del contrassegno elettronico.

Saranno emesse da DigitPA in attuazione dell'articolo 22-ter, comma 5, del Codice dell'Amministrazione Digitale. Forniranno indicazioni sui criteri di scelta e di impiego dei prodotti per la generazione del contrassegno elettronico.

Delibera DigitPA sulle modalità per presentare la domanda di iscrizione nell'elenco pubblico dei prestatori di servizi di conservazione.

Definirà le modalità con le quali i soggetti – pubblici e privati – che forniscono servizi di certificazione e intendono accreditarsi ai sensi dell'art. 44-bis del Codice, dovranno presentare domanda a DigitPA.

Linee guida per la vigilanza sui prestatori di servizi di conservazione.

Saranno emesse da DigitPA per rendere note le modalità di vigilanza. Illustreranno le modalità di verifica, la procedura che sarà seguita per le visite ispettive e le tipologie di controlli che saranno effettuati.

DPCM di definizione delle caratteristiche delle firme elettroniche

Sarà emanato, entro 12 mesi dall'entrata in vigore del Codice, un DPCM che definirà le caratteristiche della *firma digitale* e delle *firme elettroniche avanzate* anche avvalendosi di provvedimenti demandati a DigitPA. Tale scelta, utilizzata anche in passato, consente di agire rapidamente con le necessarie modifiche normative a fronte di repentine innovazioni tecnologiche.

Regole tecniche per la trasmissione di documenti attraverso la posta elettronica tra le pubbliche amministrazioni

Saranno pubblicate, entro 12 mesi dall'entrata in vigore del Codice, ai sensi dell'art 47 comma 2c, mediante DPCM che definirà le modalità di verifica della provenienza le comunicazioni tramite posta elettronica fra amministrazioni.

DPCM su soluzioni alternative per le comunicazioni con ricevuta di invio e consegna

Ai sensi dell'at.48 comma 1, sarà emesso un DPCM in merito al soluzioni tecnologiche alternative alla posta elettronica certificata che consentano la trasmissione telematica di comunicazioni con una ricevuta di invio e una ricevuta di consegna.

Regole tecniche per la realizzazione dei sistemi informativi unitari preposti alla gestione delle banche dati di interesse nazionale

Saranno emanate con DPCM attraverso il coinvolgimento dei Ministri interessati per materia, l'intesa con la Conferenza unificata ed acquisiti i pareri del Garante per la protezione dei dati personali e dell'Istituto nazionale di statistica.

Regolamenti per l'organizzazione del SPC

Saranno emanati attraverso un DPCM, su proposta del Ministro per la PA e l'innovazione e di concerto con la Conferenza unificata, e riguarderanno la determinazione dei livelli minimi dei requisiti richiesti per l'iscrizione agli elenchi dei fornitori qualificati del SPC.

Linee guida per le convenzioni per l'utilizzo dei dati pubblici

Saranno definite per consentire la diffusione e l'utilizzo delle banche dati accessibili per via telematica, consentendo alle amministrazioni titolari delle medesime di stipulare con le amministrazioni interessate convenzioni che ne regolino l'utilizzo, sentito il Garante per la protezione dei dati personali. Tali linee guida terranno conto dei modelli di interazione applicativa già previsti nell'ambito SPC e di eventuali particolari esigenze che possano suggerire altri modelli di interazione di back office.

DPCM di attuazione dell'art. 28, comma 3-bis

Sarà essere emanato, entro 12 mesi, in raccordo con le regole tecniche SPC relative all'utilizzo delle identità digitali, con DPCM, ai sensi dell'art. 28, comma 3 bis e farà riferimento alle attestazioni quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza, che potranno ai sensi del comma 3 del predetto articolo "essere rese disponibili anche in rete", in particolar modo per la parte relativa agli ordini professionali e le pubbliche amministrazioni..

Regole tecniche per estrazione di elenchi di possessori di posta elettronica certificata

Saranno emanate entro 3 mesi, in raccordo con le regole tecniche SPC relative all'utilizzo delle identità digitali, e dovranno riguardare la previsione contenuta nell'art. 6 comma 1-bis, per consentire l'accesso e l'estrazione degli elenchi contenenti i dati identificativi degli iscritti agli ordini professionali e le relative caselle di posta elettronica certificata.

Regole tecniche per l'identificazione dell'autore di un'istanza presentata tramite PEC

Saranno emanate con DPCM, riguardando la previsione introdotta dall'art. 65, comma 1, lettera c-bis) e faranno riferimento alle credenziali di posta elettronica certificata utilizzate necessarie all'identificazione dell'autore di istanze e dichiarazioni presentate in via telematica alle pubbliche amministrazioni.

Regole Tecniche per la sicurezza dei dati, dei sistemi e delle infrastrutture

Saranno emanate entro 12 mesi dall'entrata in vigore del Codice e individueranno l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture. Saranno accompagnate da un'azione di prevenzione e gestione degli incidenti di sicurezza, che sarà svolta da DigitPA anche in raccordo con strutture internazionali competenti in materia, tramite il CERT-SPC - Computer Emergency Response Team del Sistema Pubblico di Connettività - attivato dal 2008 presso DigitPA quale "*referente centrale per la prevenzione, il monitoraggio, la gestione, la raccolta dati e l'analisi degli incidenti di sicurezza*" (cit. DPCM 01.04.2008).

Regole Tecniche per il riuso modulare del software

Tali regole tecniche, che saranno emanate entro 12 mesi dall'entrata in vigore del Codice, individueranno i criteri, che consentano di verificare la presenza dei requisiti per il riuso, da rispettare nella redazione degli atti amministrativi di gara relativi a sistemi informatici o parti di essi da presentare, da parte delle Amministrazioni centrali, a DigitPA in sede di richiesta del parere di congruità. In particolare le regole tecniche dovranno facilitare la redazione di capitolati o specifiche di progetto per l'acquisizione di programmi informatici appositamente sviluppati per conto e a spese dell'amministrazione.

Linee guida sul riuso

E' opportuno perfezionare, per favorire il riuso e la più ampia diffusione delle migliori pratiche tecnologiche ed organizzative, le linee guida sul riuso pubblicate dall'allora CNIPA nel 2004, per adeguarle alla normativa vigente. Nella nuova versione delle Linee

guida sul riuso saranno inserite ulteriori check list, abachi e schemi contrattuali di riferimento per le fattispecie di riuso con gestione a carico del cedente, riuso in facility management, riuso in ASP, che indichino, sia le regole per lo sviluppo di applicativi riusabili, sia le modalità e le responsabilità di esecuzione della manutenzione correttiva, evolutiva e adeguativa.

Linee Guida sulla continuità operativa

Saranno emanate, sentito il Garante per la protezione dei dati personali, le linee guida in base alle quali le amministrazioni potranno definire, entro 15 mesi dall'emanazione del CAD, la componente di disaster recovery delle soluzioni indicate nei piani di continuità, che stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

Linee guida per le convenzioni di accesso ai dati delle amministrazioni

Entro 3 mesi dall'entrata in vigore del CAD, saranno emanate le Linee sulla base delle quali le amministrazioni redigeranno le convenzioni volte a disciplinare le modalità di accesso ai propri dati da sottoscrivere con tutte le amministrazioni interessate.

DM per la regolamentazione delle attività di pagamento

Con decreto del Ministro per la pubblica amministrazione e l'innovazione e dei Ministri competenti per materia, da emanarsi di concerto con il Ministro dell'economia e delle finanze entro 6 mesi dall'entrata in vigore del CAD, saranno regolamentate le attività di pagamento definendo i tempi di attuazione da parte delle amministrazioni interessate (la PA centrale), l'ambito di applicazione, gli elementi tecnico-organizzativi, le regole per l'esecuzione dei pagamenti informatici.

Regole tecniche per il trasferimento di fondi fra le amministrazioni

Saranno definite, entro 12 mesi dall'entrata in vigore del CAD, di concerto con i Ministri per la Funzione Pubblica, della Giustizia e dell'Economia e delle Finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia, con DPCM e disciplineranno le modalità di trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati

APPENDICE B – QUADRO DI CONFRONTO FRA I SISTEMI DI FIRMA ELETTRONICA PREVISTI NEL VECCHIO E NEL NUOVO ORDINAMENTO

Legenda delle tabelle seguenti

Immodificabilità del documento: garanzia di poter rilevare successive modifiche.

Identificazione: elementi che, liberamente valutati in giudizio, possono garantire l'identità del firmatario.

Identificazione certificata: garanzia fornita da una terza parte fidata circa l'identità del firmatario.

SSCD: Secure Signature Creation Device, trattasi del dispositivo di generazione della firma (smartcard, token USB, HSM) la cui conformità ai criteri di sicurezza prescritti dalla Direttiva europea 1999/93/CE è certificata dal preposto organismo.

HSM: Hardware Secure Module, sono dispositivi di firma, ad alta affidabilità, capaci di ospitare migliaia di chiavi per la crittografia asimmetrica.

Tipi di firma	Caratteristiche qualificanti poste dalle norme			Garanzie assolute		Valore giuridico	Bacino d'utenza
	Crittografia	Mezzo sul quale il firmatario può conservare il controllo esclusivo	Certificato qualificato	Identificazione univoca del soggetto	Immodificabilità del documento		
N1 Firma elettronica	NO	NO	NO	NO	NO	Liberalmente valutabile in giudizio	-
N2 Firma elettronica avanzata	NO	Si, in forme da individuare in sede di regole tecniche	NO	SI	SI	Art. 2702 c.c. con inversione onere della prova	Privati PA
N3 Firma elettronica qualificata	NO	Si, in forma di SSCD	SI	SI- CERTIFICATA	SI	Art. 2702 c.c. con inversione onere della prova - Art. 1350 c.c. p.ti da 1 a 12	Privati Pubblici ufficiali PA
N4 Firma digitale	SI	Si, in forme da individuare in sede di regole tecniche	SI	SI- CERTIFICATA	SI	- Art. 2702 c.c. con inversione onere della prova - Art. 1350 c.c. p.ti da 1 a 12	Privati PA

Nuovo ordinamento
D.Lgs
235/2010

Vecchio ordinamento D.Lgs 82/2005		Tipi di firma	Caratteristiche qualificanti poste dalle norme				Garanzie assolute		Valore giuridico	Bacino d'utenza
			Crittografia	Mezzo sul quale il firmatario può conservare il controllo esclusivo	Certificato qualificato	Identificazio ne univoca del soggetto	Immodificab ilità del documento			
V1	Firma elettronica	NO	NO	NO	NO	NO	Liberalmente valutabile in giudizio	Privati PA		
V2	Firma elettronica qualificata	NO	Si, in forma di SSCD	SI	SI- CERTIFICATA	SI	Art. 2702 c.c. con inversione onere della prova - Soddisfa il requisito della forma scritta - Art. 1350 c.c. p.ti da 1 a 12	Era un genere cui apparteneva l'unica specie "firma digitale"		
V3	Firma digitale	SI	Si, in forma di SSCD	SI	SI- CERTIFICATA		- Art. 2702 c.c. con inversione onere della prova - Soddisfa il requisito della forma scritta - Art. 1350 c.c. p.ti da 1 a 12	Privati Pubblici ufficia PA		

RELAZIONE FRA VECCHIO E NUOVO SISTEMA DI FIRME

V1=N1

V2=N3

V3=N3 con crittografia asimmetrica

N2 ed N4 sono dei nuovi strumenti introdotti per:

- N2 – potersi dotare di uno strumento intermedio fra la firma elettronica e la firma qualificata
- N4 – poter effettuare in sicurezza operazioni di firma da remoto

Come è evidente dal confronto fra i due sistemi, la firma elettronica qualificata del nuovo ordinamento – N3- assolve a quanto previsto per la firma digitale del vecchio ordinamento –V3.



DigitPA